WatchGuard® XCS

Extensible Content Security
v9.0 Field Guide

WatchGuard XCS
170, 370, 570, 770, 970, 1170

Notice to Users

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Document Version: 1.1

Revised: 3/30/10

Copyright, Trademark, and Patent Information

Copyright © 2010 WatchGuard Technologies, Inc. All rights reserved. All trademarks or trade names mentioned herein, if any, are the property of their respective owners.

Complete copyright, trademark, patent, and licensing information can be found in the Copyright and Licensing Guide, available online:
http://www.watchguard.com/help/documentation/

This product is for indoor use only.

ABOUT WATCHGUARD

WatchGuard offers affordable, all-in-one network and content security solutions that provide defense-in-depth and help meet regulatory compliance requirements. The WatchGuard XTM line combines firewall, VPN, GAV, IPS, spam blocking and URL filtering to protect your network from spam, viruses, malware, and intrusions. The new XCS line offers email and web content security combined with data loss prevention. WatchGuard extensible solutions scale to offer right-sized security ranging from small businesses to enterprises with 10,000+ employees. WatchGuard builds simple, reliable, and robust security appliances featuring fast implementation and comprehensive management and reporting tools. Enterprises throughout the world rely on our signature red boxes to maximize security without sacrificing efficiency and productivity.

For more information, please call 206.613.6600 or visit www.watchguard.com.

ADDRESS

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

SUPPORT

www.watchguard.com/support
U.S. and Canada +877.232.3531
All Other Countries +1.206.521.3575

SALES

U.S. and Canada +1.800.734.9905
All Other Countries +1.206.613.0895

Table of Contents

Chapter 1 WatchGuard XCS Overview 1
Chapter 2 Email Basics 9
Chapter 3 Pre-installation Tasks 13
Chapter 4 Install the WatchGuard XCS 21
Chapter 5 Mail and Network Configuration 33
Chapter 6 Anti-Virus 43
Chapter 7 ReputationAuthority 49
Chapter 8 Anti-Spam 53
Chapter 9 Directory Services 59
Chapter 10 Content Control 63
Chapter 11 Monitor the WatchGuard XCS 73
Chapter 12 System Administration 81
Chapter 13 Clustering and Queue Replication 89
Chapter 14 Web Scanning 97
Chapter 15 Available Resources 103

1 WatchGuard XCS Overview

WatchGuard XCS Overview

The WatchGuard XCS is the industry's first consolidated messaging security platform. It delivers integrated protection, control, and management for email and web content.

Firewall-level network and system security

The WatchGuard XCS delivers the most complete security available for messaging systems. The system runs on a customized and hardened Unix operating system, which prevents uncontrolled access to the system. There is no command line access and the WatchGuard XCS runs as a closed system to prevent accidental or deliberate misconfiguration by administrators, which is a common cause of security vulnerabilities.

Message delivery security

The WatchGuard XCS provides content security that enables instant-on data loss prevention, encryption and content filtering with integrated threat prevention for viruses, spam, spyware, phishing, and malware attacks, all in a secured appliance. Additionally, the WatchGuard XCS protects outbound content against unintentional or malicious data loss, privacy discrepancies and non-compliance with regulations and company policies.

The WatchGuard XCS uses a sophisticated message delivery system with several security features and benefits to make sure that the identifying information about your company's messaging infrastructure is kept private.

- For a company with multiple domain names, the system can accept, process, and deliver mail to private email servers. For a company with multiple private email servers, the system can route mail based on the domain or subdomain to separate groups of email users.
- Security features such as mail mappings and address masquerading provide the ability to hide references to internal host names.

Content controls

The WatchGuard XCS implements attachment control, content scanning, and content filtering based on pattern and text matching. These content controls prevent the following issues:

- Breaches of confidentiality
- Legal liability from offensive content
- Personal abuse of company resources
- Breaches of compliance policies

Attachment controls are based on the following characteristics:

- **File Extension Suffix** — The suffix of the file is examined to determine the attachment type, such as .exe, or .jpg.
- **MIME Content Type** — MIME (Multipurpose Internet Mail Extensions) can be used to identify the actual content type of the message.
- **Content Analysis** — The file is analyzed to look for characteristics that can identify the file type. This analysis makes sure that the attachment controls are not circumvented with a file rename.
- **Content Scanning** — Attachments such as Adobe® PDFs or Microsoft® Word documents can be analyzed for words or phrases that match a pattern filter or compliance dictionary.

Virus and spyware scanning

The WatchGuard XCS features a virus scanning engine based on Kaspersky® Anti-Virus. Both inbound and outbound email messages and web requests can be scanned for viruses and spyware. The high performance virus scanning provides a vital layer of protection against viruses for your entire organization. Automatic pattern file updates makes sure that the latest viruses and spyware are detected.

Outbreak Control

The Outbreak Control feature provides customers with zero-day protection against early virus outbreaks. For most virus attacks, the time from the moment the virus is released to the time a pattern file is available to protect against the virus can be several hours. During this period, mail recipients are vulnerable to potential threats. The Outbreak Control feature can detect and take action against early virus outbreaks to contain the virus threat.

Malformed message protection

Similar to malformed data packets used to subvert networks, malformed messages allow viruses and other attacks to avoid detection, crash systems, and lock up mail servers. The system makes sure that only correctly formatted messages are allowed into your mail systems. Message integrity checking protects your mail servers and clients and improves the effectiveness of existing virus scanning implementations.

Intercept Anti-Spam

The WatchGuard XCS provides a complete set of anti-spam features specifically designed to protect against the full spectrum of current and evolving spam threats. Intercept can combine the results of several anti-spam components to provide a better informed decision on whether a message is spam or legitimate mail with minimal false positives. These features include:

- **Spam Words** — Filters messages based on a dictionary of typical spam words and phrases that are matched against a message.
- **Mail Anomalies** — Checks various aspects of the incoming message for issues such as unauthorized SMTP pipelining, missing headers, and mismatched identification fields.
- **DNS Block List (DNSBL)** — Detects spam using domain-based lists of hosts with a poor reputation. Messages can also be rejected immediately regardless of the results of other anti-spam processing if the client appears on a DNSBL. A configurable threshold allows administrators to specify how many DNSBLs must trigger to consider the sender as unreliable.
- **URL Block List** — Detects spam by examining the URLs in a message and querying a SURBL (Spam URI Realtime Block Lists) server to determine if this URL has been used in spam messages.
- **ReputationAuthority** — The ReputationAuthority helps to identify spam by reporting a collection of metrics about the sender of a message, including their overall reputation, whether the sender is a dial-up, and whether the sender appears to be virus-infected, based on information collected from installed customer products and global DNS Block Lists. This information can be used by Intercept to reject the message, or used as part of the overall Anti-Spam decision.
- **Token Analysis** — Detects spam based on advanced content analysis using databases of known spam and valid mail. This feature is also specially engineered to effectively detect image spam.
- **Backscatter Detection** — Detects spam based on signature verification of the Envelope Sender to prevent spam bounce emails to forged sender addresses.
- **Sender Policy Framework (SPF)** — Performs a verification of a sending host's SPF DNS records to identify the source of a message.
- **DomainKeys Authentication** — Performs a verification of a sending host's DomainKeys DNS records to identify the source of a message.

ReputationAuthority

The ReputationAuthority helps to identify spam by reporting behavioral information about the sender of a message, including their overall reputation, whether the sender is a dial-up, and whether the sender appears to be virus-infected or sends large amounts of spam messages, based on information collected from installed customer products and global DNS Block Lists. Domain and Sender Reputation increases the effectiveness of ReputationAuthority by examining not only the IP reputation of a sender, but also the domain name and envelope sender information from that IP address. This information can be used by the system to either reject the message immediately or contribute to the Intercept score if a message is detected from a source with a poor reputation or numerous virus infections.

If Reputation checks are enabled, the WatchGuard XCS queries the statistics on the ReputationAuthority domain service for the sender IP address of each message received, excluding those addresses from trusted and known networks. With the information returned from ReputationAuthority, the system can make a decision about whether a message is spam or legitimate mail. A reputation of 0 indicates the sender is extremely reliable and rarely sends spam or viruses. A reputation of 100 indicates the sender is extremely unreliable and often sends spam or viruses. An IP address with no previous information from any source is assigned a value of 50.

Image spam analysis

An image spam email message typically consists of random text or no text body and contains an attachment picture (usually .gif or .jpg format) that supplies the text and graphics of the spam message. These types of spam messages are difficult to detect because the message contains no helpful text or URL characteristics that can be scanned and analyzed. The Image Spam Analysis feature performs advanced analysis of image attachments to help determine if the message is spam or legitimate mail. Similar to the other anti-spam features that detect spam characteristics in the text of a message, the Image Spam Analysis feature extracts certain characteristics of the attached image to determine if these characteristics are similar to those seen in actual spam messages.

Threat Prevention

Threat Prevention allows organizations to detect and block incoming threats in real-time. Threat types can be monitored and recorded to track client IP behavior and reputation. By examining message flow patterns, the system detects whether a sending host is behaving maliciously by sending out viruses, spam, or attempting denial-of-service (DoS) attacks. By instantly recognizing these types of patterns, Threat Prevention presents an effective solution against immediate attacks. The Threat Prevention feature can block or throttle inbound connections before the content is processed to lessen the impact of a large number of inbound messages.

Trusted and Blocked Senders List

Users can create their own personal Trusted and Blocked Senders Lists based on a sender's email address. The Trusted email addresses are exempt from the system's spam controls and allow users to trust legitimate senders, while email addresses on the Blocked Senders List are prevented from sending mail to that user through the WatchGuard XCS.

User Spam Quarantine

The User Spam Quarantine is used to redirect spam mail into a local storage area for each individual user. Users can connect to the system either directly or through a summary email to see and manage their own quarantined spam. Messages can be deleted, or moved to the user's local mail folders. Automatic notifications can be sent to end users to notify them of the existence of messages in their personal quarantine area. For large enterprises, a dedicated WatchGuard Quarantine Management Server (QMS) can be used to support up to 100,000 quarantine users and multiple domains.

Secure WebMail

Secure WebMail provides remote access support to internal mail servers. With Secure WebMail, users can get access to their mailboxes with email web clients such as Outlook® Web Access, Lotus iNotes, or the WatchGuard XCS's own web mail client. The WatchGuard XCS addresses the security issues that currently prevent deployment of web mail services and offers the following protection:

- Strong authentication (including integration with Active Directory)
- Encrypted sessions
- Advanced session control to prevent information leaks on workstations

Authentication

The WatchGuard XCS supports the following authentication methods for administrators, WebMail users, Trusted/Blocked Senders List, and Spam Quarantine purposes:

- User ID and Password
- LDAP
- RADIUS
- RSA SecurID® tokens
- SafeWord and CRYPTOCard tokens

Integrated message encryption

The Encryption Option allows organizations to easily enforce company policies and compliance regulations with the secure delivery of encrypted messages without the need for the recipient to download or install any special software. The Encryption Option uses the Cisco/PostX Registered Envelope Service which creates an encrypted message for the recipient that can be read by opening an attachment that provides access to the decrypted message.

Integrated message encryption allows users to encrypt outbound messages directly from the WatchGuard XCS without the need for a local encryption server or additional desktop software. Messages are secured until they are delivered and decrypted by the recipient of the message.

The integrated encryption engine allows the WatchGuard XCS to be configured to use the public key server for services and key-exchange related activities, or to use a local key server on the customer premises.

External encryption server support

The WatchGuard XCS integrates with external encryption servers to provide email encryption and decryption functionality. Email encryption allows individual messages to be encrypted by an external encryption server before being delivered to their destination by the WatchGuard XCS.

Incoming encrypted messages can also be sent to the external encryption server to be decrypted before the WatchGuard XCS accepts the message and delivers it to the intended recipient. This integration allows organizations to ensure that encrypted messages are still processed for security issues such as viruses, malformed mail, and content filtering and scanning.

Mail delivery encryption

All messages delivered to and from the WatchGuard XCS can be encrypted using TLS (Transport Layer Security). This includes connections to remote systems, local internal mail systems, or internal mail clients. Encrypted messages are delivered with complete confidentiality both locally and remotely.

TLS encryption can be used for the following:

- Secure mail delivery on the Internet to prevent anyone from viewing email while in transit
- Secure mail delivery across a LAN to prevent malicious users from viewing email other than their own
- Create policies for secure mail delivery to branch offices, remote users and business partners
- Supports TLS/SSL encryption for all user and administrative sessions.
- TLS/SSL is used to encrypt SMTP sessions, which effectively prevents eavesdropping and interception

Policy controls

Policy-based controls allow settings for the WatchGuard XCS's security features, including Annotations, Anti-Spam, Anti-Virus, and Attachment Control, to be customized and applied based on the group membership, domain membership, or email address of the recipient. User groups can be imported from an LDAP-based directory, and then policies can be created to apply customized settings to these groups. For example, you can set up an Attachment Control Policy to allow your Development group to accept and send executable files (.exe), and configure your Attachment Control settings for all your other departments to block this file type to prevent the spread of viruses among the general users.

Web security

The WatchGuard XCS incorporates a Web Proxy that allows the system to proxy web traffic and control access to external web sites. The system can scan web traffic using a subset of the same scanners that examine email messages to inspect the content of web traffic and downloaded files. Policy features allow specific HTTP access policies to be applied to different users, groups, and domains, and notifications for blocked connections or files can be customized and sent to the administrator and recipient.

The Web TrafficAccelerator solution provides critical web traffic enhancements, such as disk caching and streaming media support that reduce bandwidth consumption, server loads and latency to improve network performance.

Directory services

The WatchGuard XCS integrates with LDAP (Lightweight Directory Access Protocol) directory services such as Active Directory, OpenLDAP, and iPlanet, which allows you to perform the following:

- **LDAP lookup prior to internal delivery** — The system can check for the existence of an internal user through LDAP before it delivers a message. This feature allows you to reject mail to unknown addresses in relay domains, and reduces the number of attempted deliveries of spam messages for non-existent local addresses. This verification can be done directly to an LDAP server or to a cached directory stored locally on the system.
- **Group/User Imports** — An LDAP lookup determines the group membership of a user you apply policy-based controls. LDAP users can also be imported and mirrored on the system to be used for services such as the Spam Quarantine.
- **Authentication** — LDAP can be used to authenticate Web Proxy access, IMAP access, user mailbox, and WebMail logins.
- **SMTP Relay Authentication** — LDAP can be used to authenticate clients for SMTP Relay.
- **Mail Routing** — LDAP can be used to look up mail route information for a domain to deliver mail to its destination server.

System management

The WatchGuard XCS provides a complete range of monitoring and diagnostics tools to monitor the system and troubleshoot mail delivery issues. Admin sessions can also be encrypted for additional security, while comprehensive logs record all mail activity.

- **Web browser-based management** — The web browser management interface displays a live view of system activity and traffic flows. The management interface can be configured to display this information for one or many systems, including systems in a local cluster or systems that are being centrally managed.
- **Dashboard** — The WatchGuard XCS system Dashboard provides administrators with a brief statistical and graphical summary of current inbound and outbound email and web activity, to allow rapid assessment of the current status of the WatchGuard XCS.

- **Enterprise integration with SNMP** — With SNMP (Simple Network Management Protocol), the system can generate both information and traps to be used by SNMP monitoring tools. This extends the administrator's view of the WatchGuard XCS and allows notification of significant system events, including excessive traffic flows and system failures.
- **Alarms** — The system can generate system alarms that can automatically notify the administrator through email and console alerts of a system condition that requires attention.
- **Archiving** — Archiving support allows organizations to define additional mail handling controls for inbound and outbound mail. These features are especially important for organizations that must archive certain types of mail for regulatory compliance or for corporate security policies.

Clustering

The WatchGuard XCS clustering features provide a highly scalable, redundant messaging security infrastructure that enables two or more systems to act as a single logical unit to process messages with redundancy and high availability benefits. There is no theoretical limit to the size of the cluster, and systems can be easily added to the cluster to increase processing and high-availability capabilities. Clustering makes sure that the flow of traffic is not interrupted due to individual system failures. A cluster can be managed from any single system in the cluster without the need for a separate management console, and all systems in the cluster can process messages. Any configuration changes, such as Anti-Spam and Policies, are propagated to all systems in the cluster.

Reporting

The WatchGuard XCS report functionality provides a comprehensive range of informative reports that can be generated in PDF (Adobe Portable Document Format), CSV, and HTML format on demand and at scheduled times. The reports are derived from information written to the systems and message logs that are stored in the message database. Up to a month's report data can be stored and viewed online depending on message loads for a particular environment. Reports are stored on the system for online viewing, and can also be emailed automatically to the systems administrator.

In clustered environments, reports aggregate information for the entire cluster. System and resource reports display information for each system in the cluster.

For organizations that support multiple domains, per domain information can be added to the reports to provide the administrator with statistics for each hosted domain. Hosted domain reports can also be enabled that create separate reports for a specific domain that can be emailed to the administrators of each hosted domain.

Security Connection

The Security Connection provides an automated software update service that polls WatchGuard's support servers for new updates, security alerts, and Anti-Spam database updates. When new information and updates are received, a notification can be sent to the administrator.

Internationalization

The WatchGuard XCS supports internationalization for annotations, notification messages, and message database views. For example, if a message is sent to someone who is on vacation and the message used character set ISO-2022-JP (Japanese), the vacation notification sent back will be in the same character set. The message history database can also be viewed using international character sets.

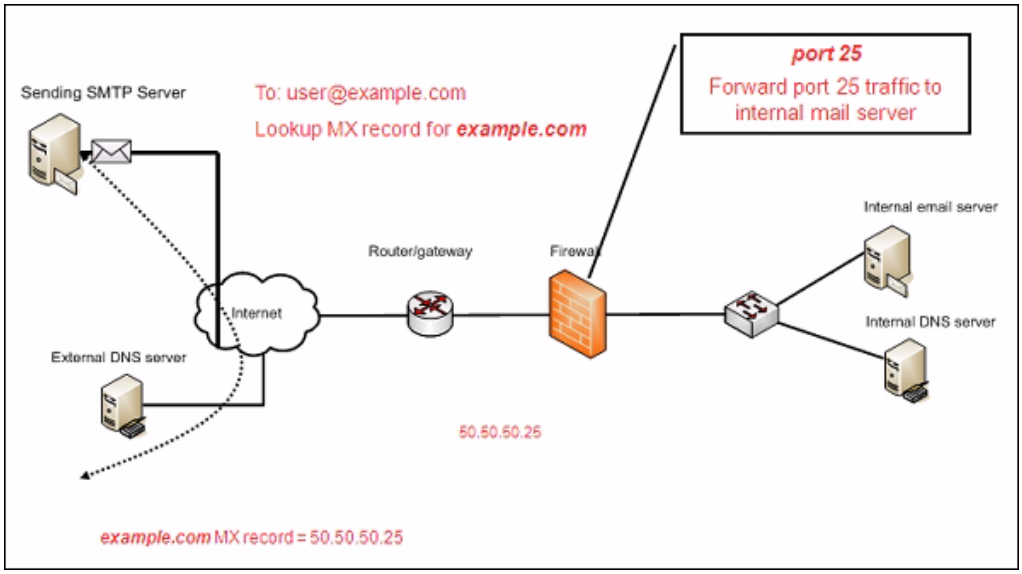
The WatchGuard XCS also supports the ISO-8859-1 (Western European Languages) based character set for dictionary-based content filtering using the Objectionable Content Filter.

2 Email Basics

Email Basics

A mail transport system consists of the following components:

- **Email clients (Mail User Agents MUA)**
  - Compose mail
  - Read mail
  - Store mail locally
- **Mail Servers (Mail Transfer Agents MTA)**
  - Relay mail to other mail servers
  - Store mail in local mailboxes



Additional network components involved in the mail delivery process:

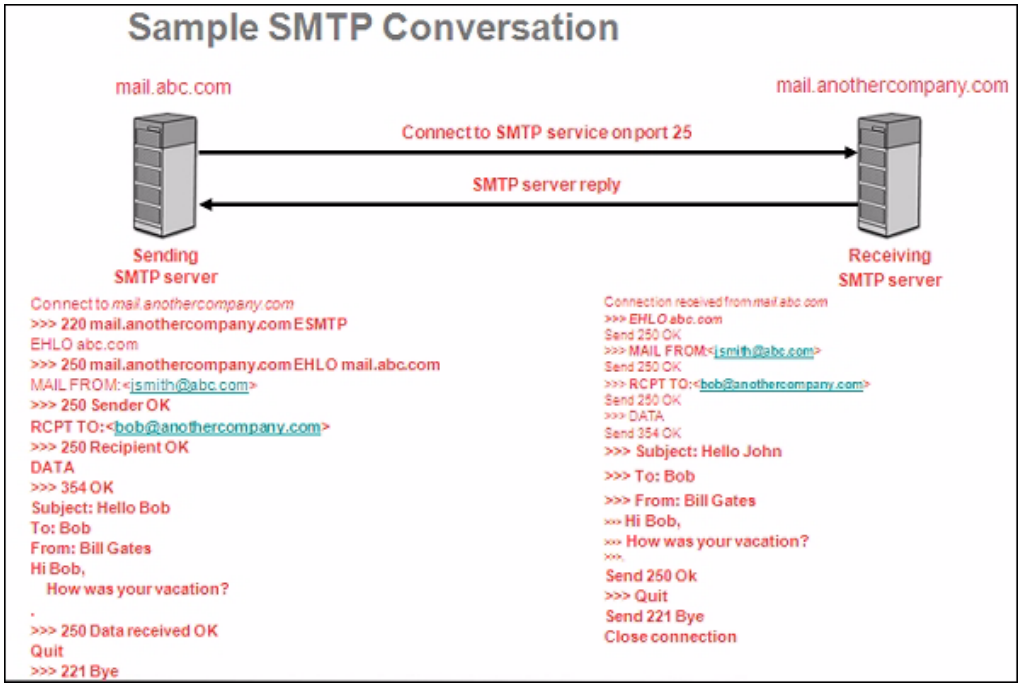
- **Domain Name Servers (DNS)**
  - Resolve hostname
  - Resolve MX records to the addresses of mail servers

- **Routers**
  - Route network packets between networks
- **Firewalls**
  - Protect the internal network
  - Prevent unauthorized access to internal network
  - Prevent unauthorized access to the external network

Send mail (SMTP)

The basic protocol used to send email is SMTP (Simple Mail Transport Protocol)

- SMTP uses a TCP-based connection on port 25
- SMTP is a simple protocol consisting of a short list of commands such as:
  - HELO or EHLO
  - MAIL
  - RCPT
  - DATA



- SMTP returns a three digit reply code to indicate success, failure or warnings, for example:
  - Service Ready (220)
  - 221 Service closing transmission channel (221)
  - Success (250 OK)
  - OK so far (354 Start mail input)
  - Temporary failure (452 mailbox full)
  - Syntax error, command unrecognized (500)
  - Permanent failure (550 user unknown)
  - Content Rejected (552)
  - Transaction failed (554)

Retrieve mail (POP and IMAP)

The following two protocols are typically used by mail clients to retrieve email:

- POP (Post Office Protocol) uses a TCP-based connection on port 110, and is used to retrieve messages from a shared message store for offline processing
- IMAP (Internet Message Access Protocol) uses a TCP-based connection port 143, and is used to access messages in a shared message store

Email message parts

The following is an example of a typical mail message:

Anatomy of an Email Message
HELO mail.watchguard.com
MAIL FROM: yourbestfriend@yahoo.com
RCPT TO: user@watchguard.com
DATA
envelope
RECEIVED: from mail.watchguard.com (mail.watchguard.com [10.10.1.88])
by server.watchguard.com (8.11.1/8.11.1) with ESMTP id h4DKCF517028
for <user@server.watchguard.com>; Tue, 13 May 2003 16:12:15 -0400 (EDT)
(envelope-from anybody@anywhere.com)
RECEIVED: by mail.watchguard.com (watchguard WatchGuard XCS) id 4D627D2DF1; Tue, 13 May 2003 16:12:15 -0400 (EDT)
DELIVERED-TO: user@watchguard.com
RECEIVED: from fake (server.watchguard.com [10.10.0.2])
by mail.watchguard.com (watchguard WatchGuard XCS) with SMTP id 9056D2DE0
for <user@watchguard.com>; Tue, 13 May 2003 16:11:06 -0400 (EDT)
SUBJECT: Read me please
TO: user@watchguard.com
FROM: yourbestfriend@yahoo.com
MESSAGE-ID: 20030513201106.39056D2DE0@mail.watchguard.com
DATE: Tue, 13 May 2003 16:11:06 -0400 (EDT)
<blank line>
headers
Hello, how are you?
body

Envelope

- The message envelope is never seen by the end user
- It is used internally by the MTA to route the message
- Contains the sender and recipient address

Headers

- Each header is transmitted as a single line of text
- Date, From, To are mandatory headers
- Optional headers include: Subject, Cc, Reply-To, Received, Message-ID
- Header beginning with "*X-*" are for custom usage

Message body

- The message body is the actual content of the email message
- Must be in plain text
- Binary content must be encoded into ASCII text
- Separated from the headers by a single blank line

3 Pre-installation Tasks

WatchGuard XCS Deployments

The WatchGuard XCS is designed to be situated between internal email servers and clients, and external servers on the Internet so that there are no direct connections between external and internal systems.

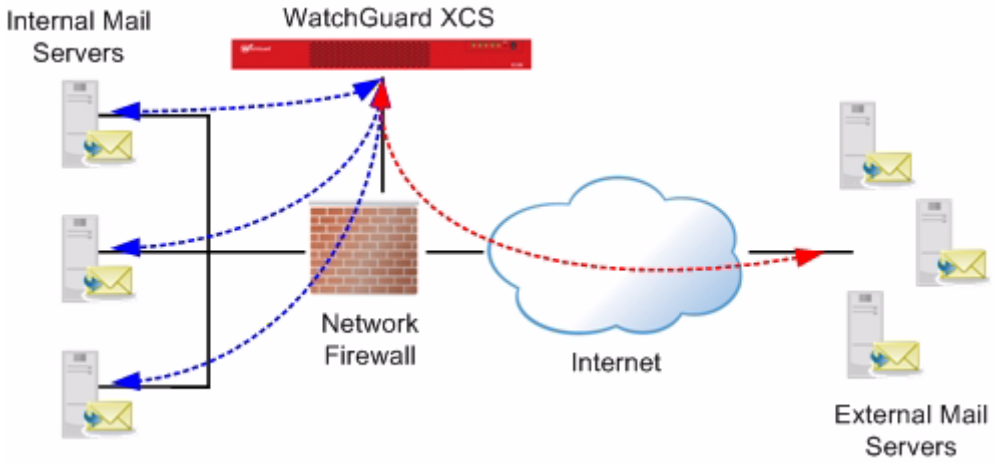
The WatchGuard XCS is typically installed in one of three locations:

- On the DMZ (Demilitarized Zone) of a network firewall
- In parallel with a network firewall
- Behind the existing firewall on the internal network

Messaging traffic is redirected from either the external interface of the network firewall or from the external router to the system. When the message is accepted and processed, the system initiates a connection to the internal mail servers to deliver the messages.

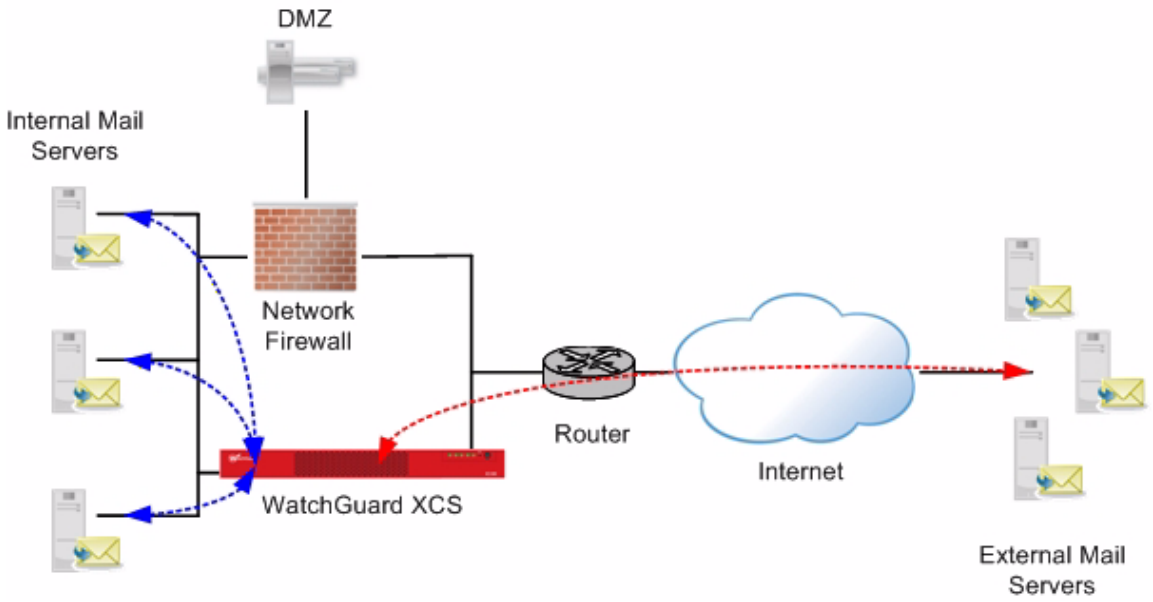
WatchGuard XCS on the DMZ of a network firewall

The most common deployment strategy for the WatchGuard XCS is to be situated on the DMZ of a network firewall. This type of deployment prevents any direct connections from the Internet to the internal mail servers, and makes sure the WatchGuard XCS is located on a secure network behind the firewall.



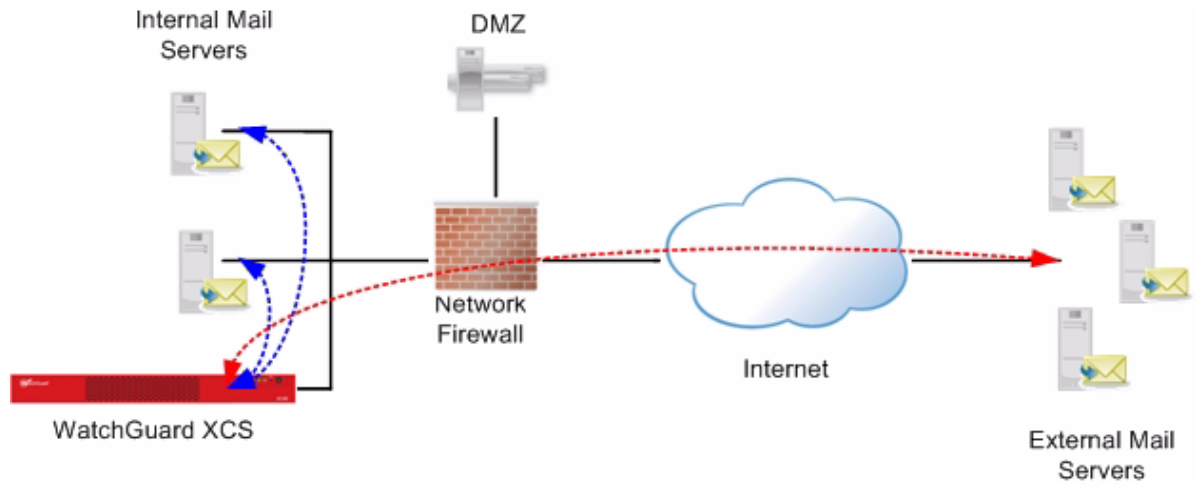
WatchGuard XCS in parallel with a network firewall

You can deploy the WatchGuard XCS in parallel with an existing network firewall as another secure method of deployment. The system's inherent firewall security architecture eliminates the risk associated with deployment of the appliance on the perimeter of a network. This parallel deployment eliminates any messaging traffic on the network firewall and decreases its overall load. A second network interface must be configured to connect to the Internet-facing network.



WatchGuard XCS on the internal network

The WatchGuard XCS can also be deployed on the internal network. Although this configuration allows a direct connection from the Internet into the internal network, it is a legitimate configuration when required by existing network resources.



Before You Begin

Before you begin the installation process, make sure you do the tasks described below.

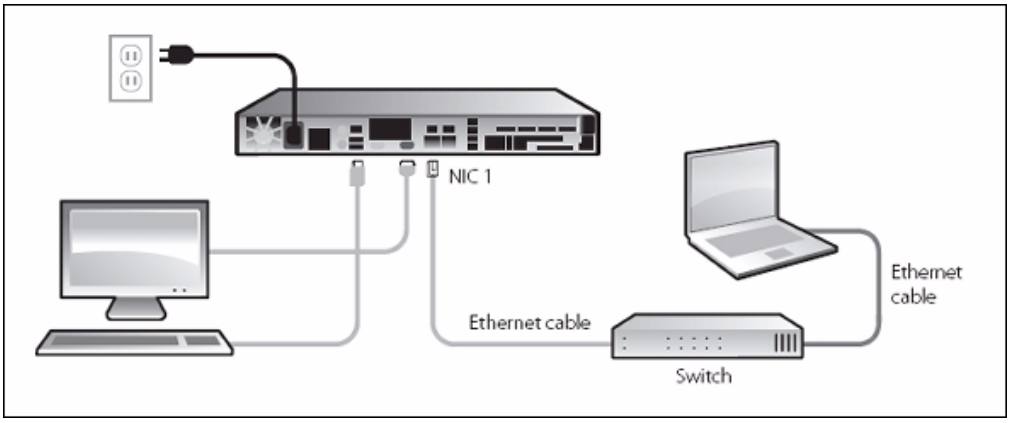
Verify basic components

Make sure that you have these items:

- A computer with an Ethernet network interface card and a web browser installed
- WatchGuard XCS device
- Keyboard and monitor
- Ethernet cables
- Power cables

Hardware installation

Use the instructions in the Quick Start Guide and Hardware Setup Guide included in the shipping box to install the WatchGuard XCS device in an equipment rack and connect the monitor, keyboard, and network interfaces.



Connect the monitor and keyboard

For the initial installation, a monitor and keyboard (USB or PS/2) are required to operate the system console. After the initial console configuration is complete, the system can be managed remotely with the Web UI.

Connect the network interfaces

Before installation, make sure that at least one of the network interfaces is physically connected to the network. This will help you to more easily confirm that you have correctly identified the system on the network and verify connectivity.

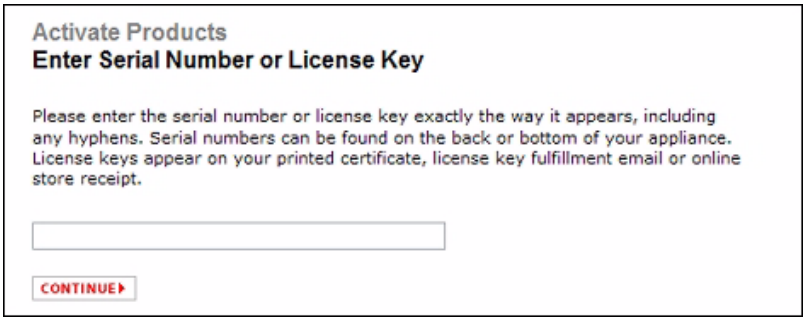
For all hardware models, we recommend that you use the first onboard Ethernet network interface (NIC 1) on the left of the device during the installation process as the LAN-facing interface. This is the first default interface assigned by the system during the installation. After the installation is complete, you can configure an additional network interface as your external Internet-facing interface.

Get a feature key

A feature key is a license that enables you to activate your purchased feature set on your WatchGuard XCS. You must register the device serial number on the WatchGuard LiveSecurity® web site and retrieve your feature key.

To activate a serial number and obtain a feature key:

1. Open a web browser and go to https://www.watchguard.com/activate.
   If you have not already logged in to LiveSecurity, the LiveSecurity Log In page appears.
2. Enter your LiveSecurity user name and password.
   The Activate Products page appears.
3. Enter the serial number for the product as it appears on your hardware device, including the hyphens.


Activate Products
Enter Serial Number or License Key
Please enter the serial number or license key exactly the way it appears, including any hyphens. Serial numbers can be found on the back or bottom of your appliance. License keys appear on your printed certificate, license key fulfillment email or online store receipt.
CONTINUE

4. Click **Continue**.
   The Choose Product to Upgrade page appears.
5. In the drop-down list, select the WatchGuard XCS device.
6. Click **Activate**.
   The Retrieve Feature Key page appears.
7. Copy the full feature key to a text file and save it on your computer.
8. Click **Finish**.

Gather network addresses

Gather the following information about your networking environment before you start the installation. Record your network information in the following table before you configure your WatchGuard device.

Hostname
The hostname assigned to the WatchGuard XCS, such as `hostname` in the FQDN (Fully Qualified Domain Name) `hostname.example.com`.

Domain Name
The domain name associated with the assigned hostname. This is typically the domain that messages are being processed for, such as `example.com`.

Internal IP Address
Select an IP address for the internal LAN-facing trusted network interface. This address is used to connect remotely to the system with the Web UI.

External IP Address
Select an IP address for the external network interface. This is the WAN-facing interface that is connected to a public network such as the Internet.

Subnet Mask
The subnet mask for the IP addresses you have chosen.

Gateway Address
The default gateway for the system. In most cases this is your network router.

Mail Domains
The mail domains the WatchGuard XCS will be processing messages for.

Internal Mail Servers
The domain name or IP address of your internal mail servers that will be receiving and sending messages through the WatchGuard XCS.

Optional Network Cards
The IP address, Subnet Mask, and Gateway Address for any additional network cards required by your choice of deployment.

DNS Servers
The addresses of your DNS (Domain Name Service) name servers, including a primary and secondary server.

NTP Servers
The addresses of your NTP (Network Time Protocol) servers for time synchronization, including a primary and secondary server.

Table 1: Basic Network Settings		Example
Hostname	_____	hostname
Domain Name	_____	example.com
Internal IP Address (LAN, Trusted)	_____._____._____._____	10.0.1.10
Subnet Mask	_____._____._____._____	255.255.0.0
External IP Address (WAN)	_____._____._____._____	100.100.100.10

Table 1: Basic Network Settings		Example
Subnet Mask	_____._____._____._____	255.255.0.0
Gateway Address	_____._____._____._____	10.0.1.1
Mail Domains	_____ _____ _____	example.com example1.com
Internal Mail Servers	_____._____._____._____ _____._____._____._____ _____._____._____._____	10.0.2.25 10.0.3.25
Optional Network Cards	_____._____._____._____ _____._____._____._____	10.0.5.10
DNS Servers	_____._____._____._____ _____._____._____._____	10.0.2.53 10.0.3.53
NTP Servers	_____._____._____._____ _____._____._____._____	10.0.2.123 10.0.3.123

Additional configuration

When you have decided on a deployment strategy, gather the following information about your environment:

- Determine which ports must be opened on the network firewall (if the system is deployed behind a firewall)
- Determine appropriate DNS settings for mail routing
- Identify changes required to the internal mail servers to route outbound email messages through the WatchGuard XCS

Network firewall configuration

For the WatchGuard XCS to process messages effectively when located behind a network firewall, various networking ports must be configured on the network firewall.

This table describes the list of ports required for each service. If you do not use some of the features shown in the table, the corresponding ports can remain closed:

Port	Description	From Internet To XCS	From XCS To Internet	From Internal Network to XCS	From XCS To Internal Network	Protocol
21	FTP for System Backups				X	TCP
22	SCP (Backup or Offload)				X	TCP
25	SMTP (standard port for sending and receiving of mail)	X	X	X	X	TCP
53	DNS and ReputationAuthority Queries		X		X	TCP/UDP
80	Anti-Virus Updates (also requires port 443)		X			TCP
80	URL Categorization Updates		X			TCP
80	Web Mail Access (OWA, iNotes, etc.) See port 443 for Secure WebMail access.	X		X		TCP
110	POP3	X		X		TCP
123	Network Time Protocol (NTP)		X		X	UDP
143	IMAP Proxy	X		X		TCP
161	SNMP			X		UDP
162	SNMP Traps				X	UDP
389	LDAP				X	TCP
443	WatchGuard XCS Software Updates		X			TCP
443	Anti-Virus Updates (also requires port 80)		X			TCP
443	Secure Web Mail Access	X		X		TCP
443	Web UI connections	X		X		TCP
443	ReputationAuthority Statistics Sharing		X			TCP

Port	Description	From Internet To XCS	From XCS To Internet	From Internal Network to XCS	From XCS To Internal Network	Protocol
514	Syslog				X	UDP
636	LDAPS				X	TCP
993	Secure IMAP	X		X		TCP
995	Secure POP3	X		X		TCP
1812	RADIUS Server				X	UDP
5500	RSA Secure ID ACE Server				X	UDP
10101	Support Access	X	X			TCP
10106	Centralized Management	X	X	X	X	TCP

DNS configuration for mail routing

DNS services are used to route mail messages from the Internet to the WatchGuard XCS. DNS configurations can be quite complex and are usually dependant on the networking environment of your organization.

These instructions represent the minimum changes required for mail routing:

- Add an MX (mail exchanger) record to your DNS configuration to forward incoming messages to the WatchGuard XCS:
  ```
  example.com. IN MX 0 hostname.example.com
  ```
- Add an "A" record to resolve the domain name to an IP address:
  ```
  hostname.example.com. IN A 10.0.1.10
  ```
- Add a PTR record to allow reverse look-ups to succeed and prevent messages sent from the WatchGuard XCS being marked as suspected spam:
  ```
  10.1.0.10.in-addr.arpa. IN PTR hostname.example.com
  ```
- Consider keeping an MX record with a higher preference pointed at your current mail server during the integration phase. If the WatchGuard XCS is taken out of service, the messages automatically route directly to the mail server. You must delete this entry before you move to a production environment as spammers could find this alternate route and bypass the WatchGuard XCS.
  ```
  example.com. IN MX 10 mailserver.example.com
  ```

Outbound mail routing

While DNS entries are required to route inbound messages through the WatchGuard XCS, changes are required to the existing internal mail servers to route outbound messages through the WatchGuard XCS.

After the installation is complete, all internal systems must be configured to use the WatchGuard XCS for delivery. This allows outbound message content to be processed for attachments and suspect files to prevent the spread of viruses introduced locally, and improves the spam detection capabilities of the system's Anti-Spam features.

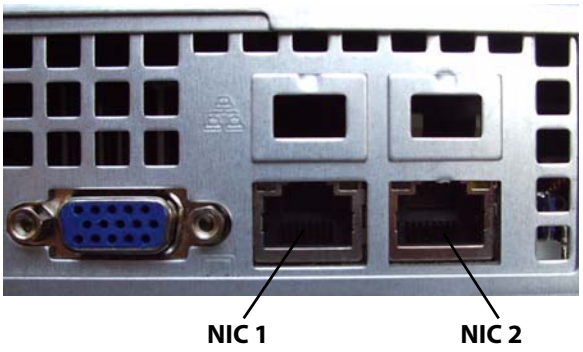
See "Modify Internal Mail Servers for Outbound Mail" on page 37 for detailed information about how to configure an internal mail server.

4 Install the WatchGuard XCS

Console Installation

To install the system from the console:

1. Unpack the system, cables, and documentation from the shipping carton.
2. Connect the power cable to the system and a power source, preferably via a UPS (Uninterruptible Power Supply).
3. Connect a monitor and keyboard to the system.
   You can use a USB or PS/2 type keyboard.
4. Connect the first onboard Ethernet network interface on the left of the device (NIC 1) to the network.
   During the initial installation, only the internal LAN-facing network interface must be connected to connect to the system with a web browser. Additional network interfaces, if required, can be configured after the installation.



5. To power on the system, press the power button on the front of the device.

6. These options are displayed at startup:

   - **F1 Install** — The **Install** option is used to reinstall the system to factory default settings.
   - **F2 System** — The **System** option loads the existing installation. This option is chosen by default after a few seconds.
7. Press **F2 System** or wait for the option to be automatically selected.

Extensible Content Security 9.0 Installation and Configuration
The Extensible Content Security software has been loaded onto your system's hard disk. The next step is to configure the available disk space to match your requirements.
Press <RETURN> to continue
Software Installation
Extensible Content Security 9.0

8. Press **Return** or **Enter** to continue with the installation.
9. Select the disk installation type.

Installation Type
You can select Auto Installation which will use reasonable defaults for all configuration choices, or you can perform a Custom Installation which will allow you to specify individual configuration choices.
Select installation type: <Auto> <Custom>
<esc> to quit
Software Installation
Extensible Content Security 9.0

   - **Auto** — Default values for disk space allocation for log file storage, message storage, backup area, and database area are used.

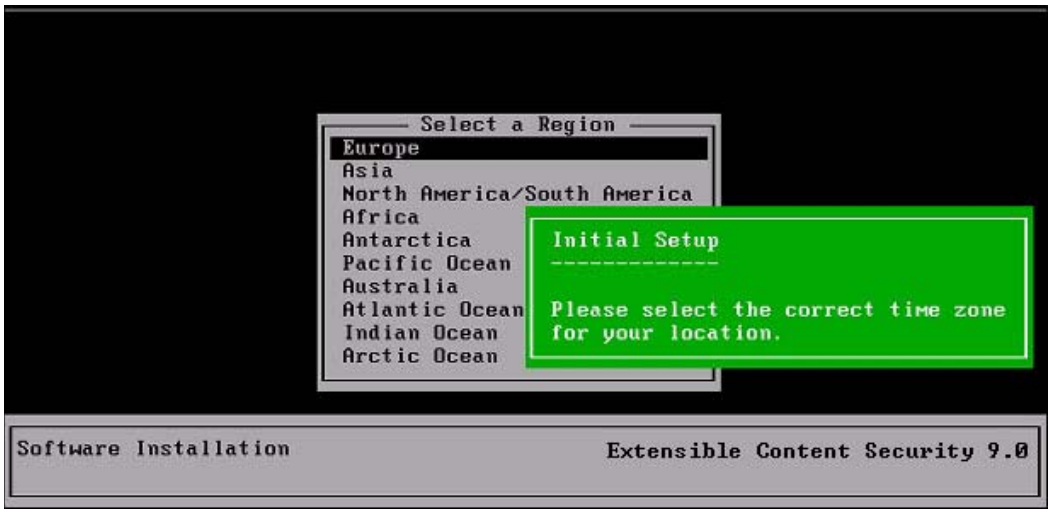
- **Custom** — To edit the default space allocation values, select **Custom**.

  A custom partition may be required if you want to increase the size of the backup partition to accommodate large backups with log file and report data.
  - The hard disk is detected and identified. Select **Continue**.
  - Select **Edit** to edit the disk layout.
    Use the arrow keys to move between fields.
  - Press **Enter** to use the displayed action such as "+ 100" or "+ 1000".
    The values are in megabytes. You must decrease the amount allocated to one file system before you increase another.
  - When finished, select **Done**, and then **OK** to exit the disk layout screen.

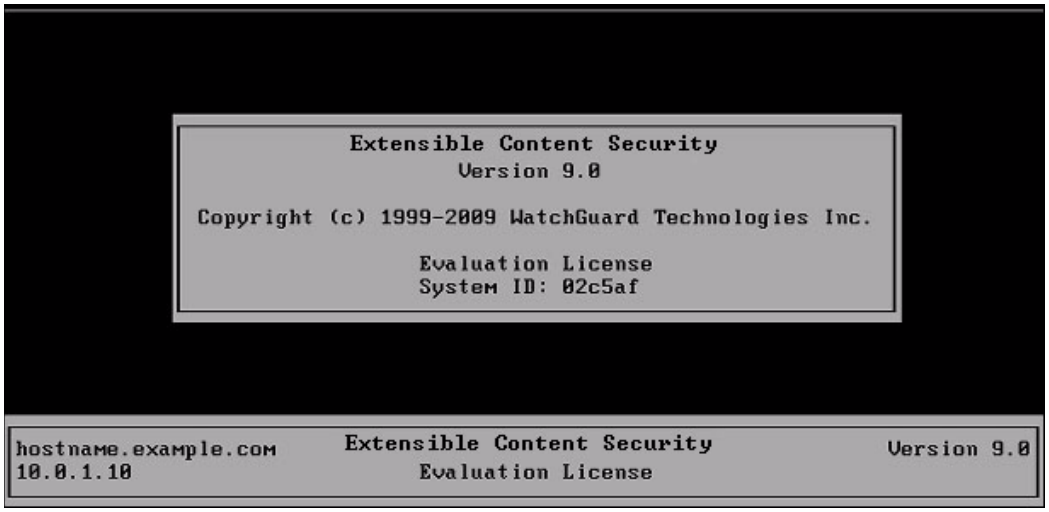
10. Select **Yes** to erase the hard disks.
11. Click **OK** to configure a network interface.
    You use this network interface and IP address to connect to the system with a web browser when the console installation is complete. We recommend that you configure the internal LAN interface first and use this interface to complete the installation process. Use the first onboard Ethernet connector on the left of the device (NIC 1). You can configure additional interfaces with the network settings configuration page when the installation is complete.

12. Select the **Interface** to configure, such as **em0** in this example.
    This is the first onboard Ethernet connector on the left of the device (NIC 1).
13. Type the **Hostname** for the system, such as `hostname` in the fully qualified domain name `hostname.example.com`.
14. Type your **Domain**, such as `example.com`.
15. Type the **IP Address** for this interface, such as `10.0.1.10`.
16. Type the **Subnet mask**, such as `255.255.0.0`.
17. Type the **Gateway** (typically the router) for your network, such as `10.0.1.1`.
18. Type the IP address of your DNS **Name Server**, such as `10.0.2.53`.
19. Select **OK** to continue.

20. Set the region and time zone appropriate for your location.



21. The initial configuration is complete and the system console screen is displayed.
You see a message warning "Mail System is stopped!". This message is normal because messaging services have not been started yet.



You must now connect to the system with a web browser to continue with the installation.

Start the Web UI Setup Wizard

To continue configuration, you must connect to the system with the Web UI to run the Setup Wizard.

Supported web browsers

The following web browsers are supported for use, at a minimum screen resolution of 1024x768:

- Internet Explorer 6 (Windows XP, Windows 2000, Windows 2003)
- Internet Explorer 7 (Windows XP, Windows 2000, Windows 2003, Windows Vista)
- Firefox 3.0 and greater (Windows, Linux, Mac)

Connect to the Web UI

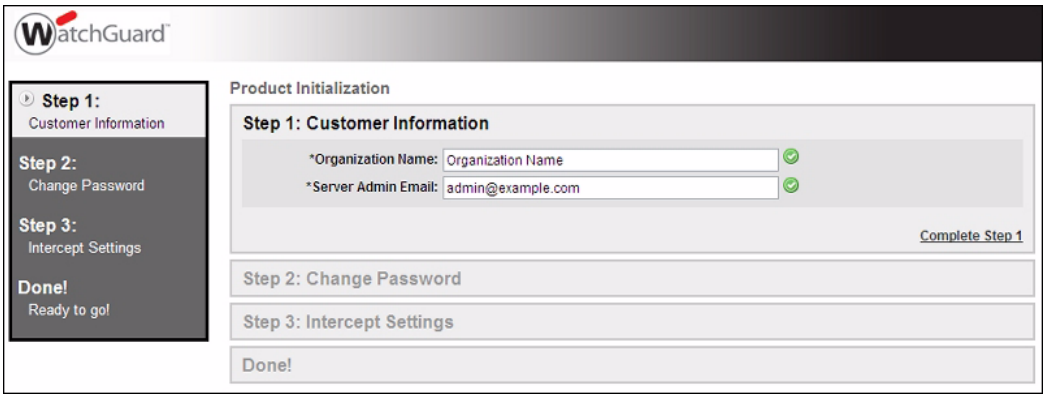
To connect to the Web UI:

1. Launch a web browser on your computer and enter the IP address of the WatchGuard XCS as the URL in the location bar, such as `http://10.0.1.10`
   The login screen is displayed.

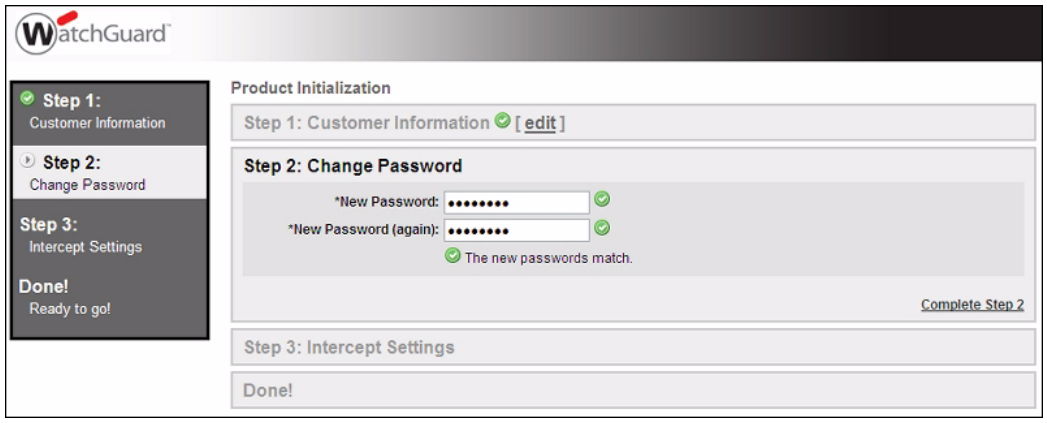
A security certificate notification appears in the browser because the system uses a self-signed certificate. It is safe to ignore the warning (Internet Explorer) or to add a certificate exception (Mozilla Firefox).

2. Type the default **Username** and **Password**.
   When you connect to the system for the first time after installation, the default settings are **admin** for the Username, and **admin** for the Password.

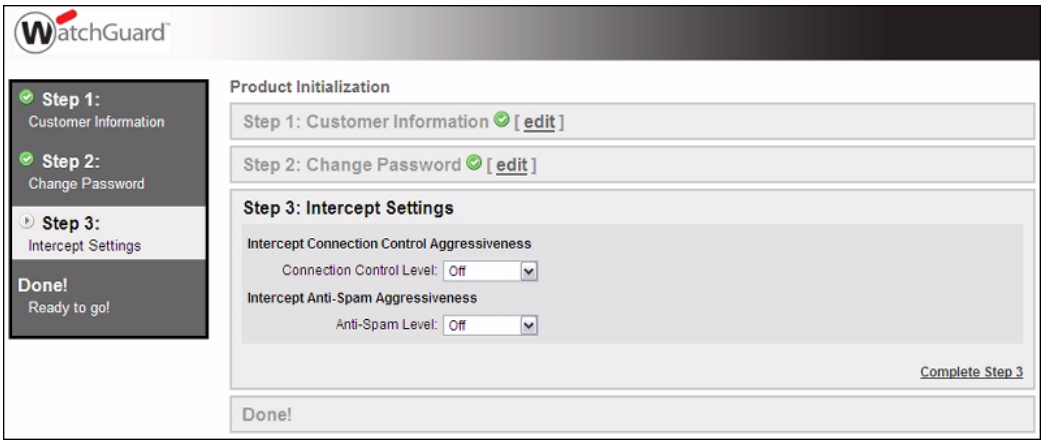
3. Type an **Organization Name** and **Server Admin Email** address for this system.
   The server admin email address will receive all system alerts and notifications.



4. Click **Complete Step 1** to continue.
5. You must change the default admin password after you log in.
   We recommend that you choose a secure password of at least 8 characters in length and include a mixture of upper and lowercase alphabetic characters, numbers, and special characters.



6. Click **Complete Step 2** to continue.
7. Specify the initial level of aggressiveness for the system's **Intercept Connection Control** and **Intercept Anti-Spam**.



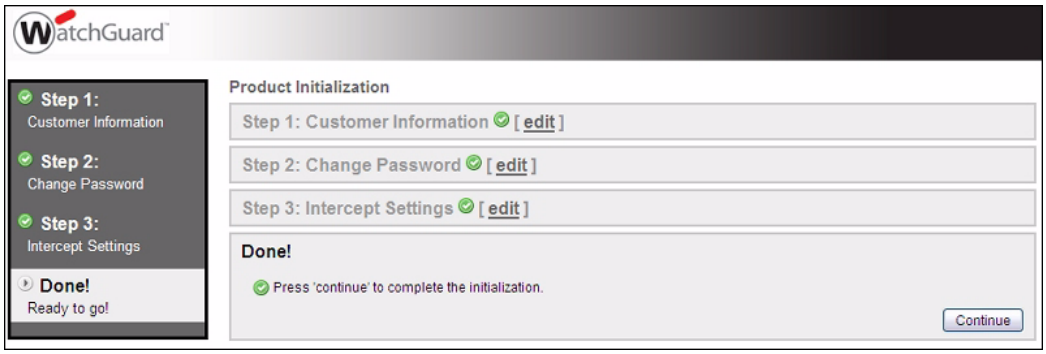
The following table describes the levels of aggressiveness for **Intercept Connection Control**:

Feature	Lenient	Standard	Aggressive
Reject on unknown sender domain	X	X	X
Reject on missing sender MX			
Reject on non FQDN sender	X	X	X
Reject on unauth pipelining	X	X	X
Reject on missing addresses			
Reject on missing reverse DNS			
Reject on ReputationAuthority Reputation		X (Threshold: 99)	X (Threshold: 85)
Reject on infection (ReputationAuthority)			X
Reject connections from dial-ups (ReputationAuthority)			X
Reject on DNSBL		X (Threshold: 2)	X (Threshold: 1)

The following table describes the levels of aggressiveness for **Intercept Anti-Spam**:

Intercept Option	Lenient	Standard	Aggressive
Certainly Spam	Modify Subject Header	Reject	Reject
Probably Spam	Modify Subject Header	Modify Subject Header	Modify Subject Header
Maybe Spam	Just Log	Just Log	Modify Subject Header
Decision Strategy	Heuristic 1	Heuristic 1	Heuristic 2
Spam Words	X	X	X
Mail Anomalies		X	X
DNS/URL Block List	X	X	X
ReputationAuthority		X	X
Token Analysis	X	X	X
SPF			X
DomainKeys		X	X

8. Click **Complete Step 3** to continue.



9. Click **Continue** to complete the installation.
   You must add a feature key for your system and configure your basic message delivery settings, as detailed in the following sections, before you start the messaging system.

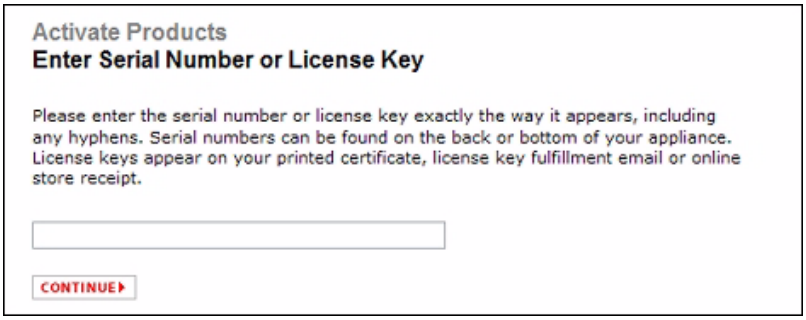
Feature Key

A feature key is a license that enables you to activate your purchased feature set on your WatchGuard XCS. You must register the device serial number on the WatchGuard LiveSecurity web site and retrieve your feature key before you add it to the WatchGuard XCS.

Get a feature key from LiveSecurity

To retrieve a feature key from the LiveSecurity web site:

1. Open a web browser and go to *https://www.watchguard.com/activate*.
2. If you have not already logged in to LiveSecurity.
   The LiveSecurity Log In page appears.
3. Enter your LiveSecurity user name and password.
   The Activate Products page appears.

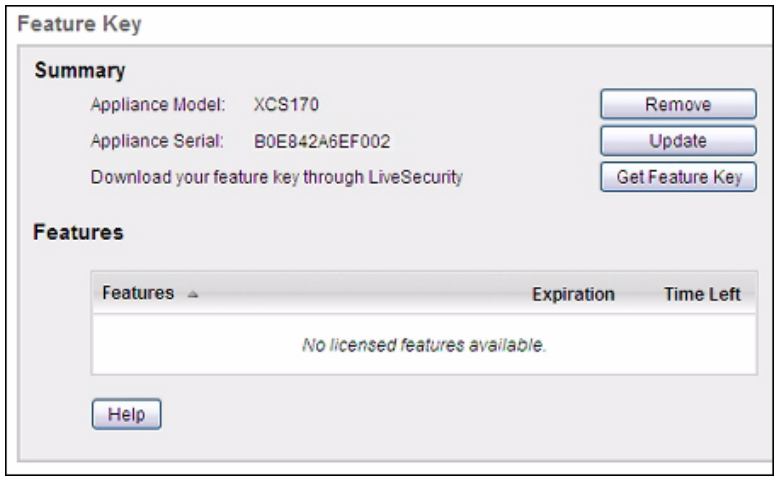

Activate Products
Enter Serial Number or License Key
Please enter the serial number or license key exactly the way it appears, including any hyphens. Serial numbers can be found on the back or bottom of your appliance. License keys appear on your printed certificate, license key fulfillment email or online store receipt.
CONTINUE

4. Enter the serial number for the product as it appears on your hardware device, including the hyphens.
5. Click **Continue**.
   The Choose Product to Upgrade page appears.
6. In the drop-down list, select the WatchGuard XCS device.
7. Click **Activate**.
   The Retrieve Feature Key page appears.
8. Copy the full feature key to a text file and save it on your computer.
9. Click **Finish**.

Add a feature key to the WatchGuard XCS

To install a new feature key:

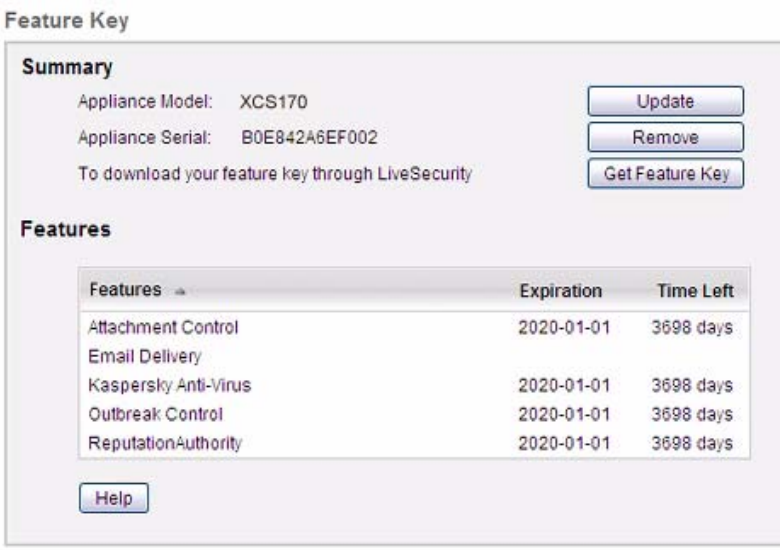
1. Select **Administration > System > Feature Key**.
   The Feature Key page appears.



2. Click **Update**.
   The Update Feature Key page appears.

3. Copy the text of the feature key file and paste it in the text box.

4. Click **Update Key**.
   The Feature Key page reappears with the new feature key information.

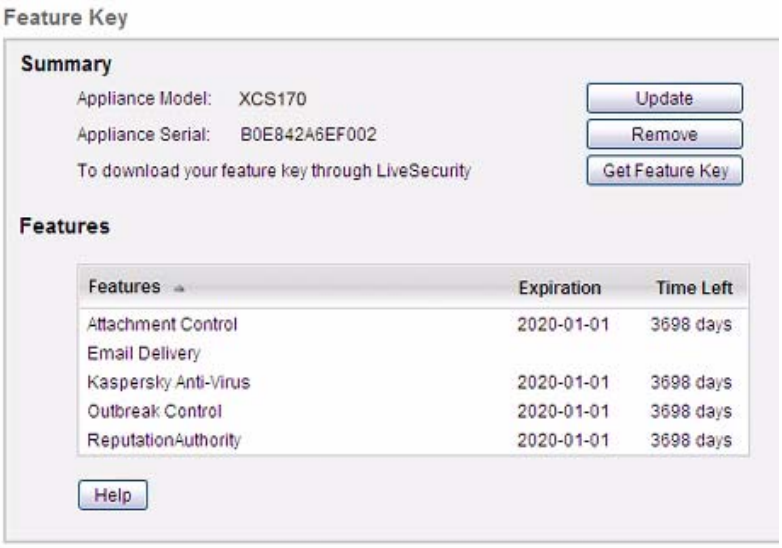


Update a feature key

If you already have a LiveSecurity login and your WatchGuard device serial number is registered, you can update your feature key automatically from the LiveSecurity site.

To update a feature key:

1. Select **Administration > System > Feature Key**.
   The Feature Key page appears.



2. Click **Get Feature Key**.
   Your feature key is downloaded from the LiveSecurity site and automatically updated on your system.

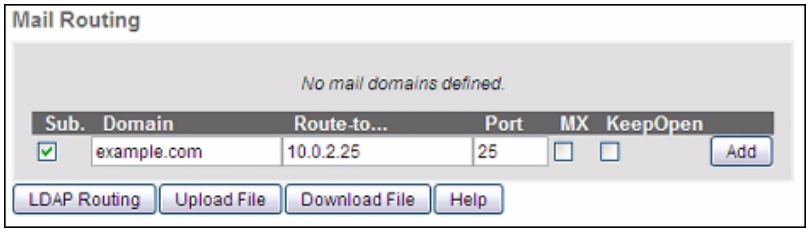
5 Mail and Network Configuration

Configure Mail Routing

You must configure the domains to accept mail for and identify the destination mail servers to route the messages to.

To add and configure mail routes:

1. Select **Configuration > Mail > Routing**.



2. Select the **Sub** option to accept and relay mail for subdomains of the specified domain.
3. Enter the **Domain** for which mail is to be accepted, such as `example.com`.
4. Enter the **Route-to** address for the server to which mail will be delivered, such as `10.0.2.25`.
   This is the address of your internal mail server.
5. Enter the **Port** on which to deliver mail to this server.
   The default is SMTP port 25.
6. Select the **MX** option if you need to look up the mail routes in DNS before delivery.
   It is not necessary to select this item unless you use multiple mail server DNS entries for load balancing and failover purposes. When you select the MX option, DNS sends the request to the next mail server in the list. If this option is not enabled, MX records are ignored.
7. Select the **KeepOpen** option to make sure that each mail message to the domain is not removed from the active queue until delivery is attempted, even if the preceding mail failed or was deferred.
   Select this option to make sure that local mail servers receive high priority.

The KeepOpen option should only be used for domains that are usually very reliable. If the domain is unavailable, it can cause system performance problems due to excessive error conditions and deferred mail.

8. Click **Add**.

9. Repeat the procedure for any additional domains and mail servers.

Upload mail routes

A list of domains can also be uploaded in one text file. The file must contain comma or tab separated entries in the form:

`[domain],[route],[port],[ignore_mx],[subdomains_too],[keepopen]`

For example:

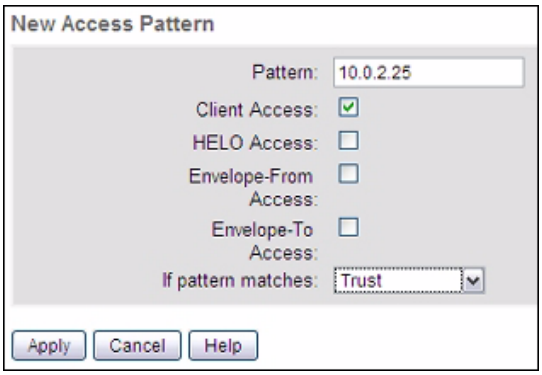
`example.com,10.0.2.25,25,on,off,off`

The file (domains.csv) should be created in .csv file format with a text editor. We recommend that you download the domain file first by clicking **Download File**, edit it as required, and upload it with the **Upload File** button.

Trust Internal Mail Servers

To allow internal mail systems to relay mail outbound through the WatchGuard XCS, you must configure a Specific Access Pattern. A Specific Access Pattern makes sure that your mail servers and their messaging traffic is trusted and not processed for spam. To configure a Specific Access Pattern:

1. Select **Configuration > Mail > Access**.
2. Click **Add Pattern**.



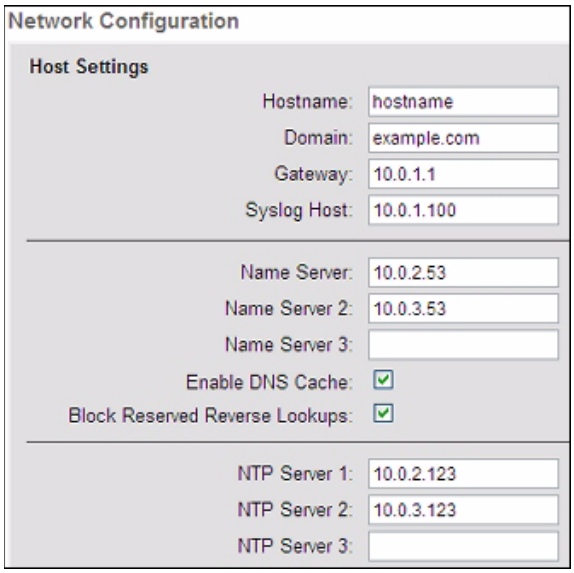
3. Enter the IP address of the internal mail server, such as `10.0.2.25`.
   You must configure a separate access pattern for each internal mail server.
4. Select **Client Access**.
5. Set the **if pattern matches** field to **Trust**.
6. Click **Apply**.

Configure Network Settings

The basic networking information to get the WatchGuard XCS operational on your network is configured during installation. To do more advanced network configuration and to configure other network interfaces, you must use the network interface settings dialog box.

To configure network settings:

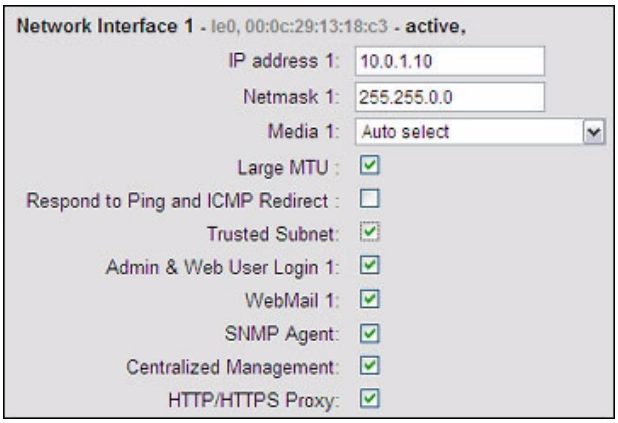
1. Select **Configuration > Network > Interfaces**.
   The network configuration page appears.



2. The **Hostname**, **Domain**, and **Gateway** were configured during the initial installation and can be modified on this page.
   - Type the **Hostname** (not the full domain name) of the system, such as `hostname` in the domain name `hostname.example.com`.
   - Type the **Domain** name, such as `example.com`.
   - Type the IP address of the default **Gateway** for this system.
     This is usually the external router connected to the Internet or the network firewall's interface if the system is located on the DMZ network.
3. Type an optional IP address or hostname for a **Syslog Host** server that will receive logs from this system.
   A syslog host collects and stores log files from many sources.
4. Type the address of your primary and secondary DNS **Name Servers**.

   The primary DNS Name Server was configured during the initial installation. At least one DNS Name Server must be configured for hostname resolution and we recommend that you specify secondary name servers in case the primary DNS server is unavailable.
5. Keep the **Enable DNS Cache** and **Block Reserved Reverse Lookups** options enabled.
6. Type the address of your primary and secondary **NTP Servers** to synchronize your system time with a reliable external time source.
   NTP (Network Time Protocol) is critical for accurate timekeeping for the system. Secondary NTP servers should be specified in the event the primary NTP server is unavailable.

7. You can configure any other additional network interfaces you require.
   For each network interface, you can configure the following options:



8. Type an **IP Address**, such as `10.0.1.10`.
9. Type the **Netmask** for this interface, such as `255.255.0.0`.
10. Select the **Media** type of the network card.
    Use Auto select for automatic configuration.
11. Enable the **Large MTU** option that sets the MTU (Maximum Transfer Unit) to 1500 bytes.
    This option can improve performance connecting to servers on the local network. The default MTU is 576 bytes.
12. Select any other options required for this interface:
    - Select the **Respond to Ping and ICMP Redirect** option to allow ICMP ping requests to this interface.
      This option allows you to perform network connectivity tests to this interface, but causes this interface to be more susceptible to denial of service ping attacks.
    - Select the **Trusted Subnet** option to consider all hosts on this subnet trusted for relaying and Anti-Spam processing.
      This setting should only be enabled on your internal LAN-facing interface that accept trusted mail.
    - Select the **Admin and Web User Login** option to allow access to this interface for administrative purposes, such as Tiered Admin users and Web users.
      This setting should only be enabled on your internal LAN-facing interface.
13. Click **Apply**.
    You must reboot the WatchGuard XCS device to apply the network settings.

Modify Internal Mail Servers for Outbound Mail

Changes are required to your existing internal mail servers to route outbound mail through the WatchGuard XCS. You must configure your internal mail servers to use the hostname or IP address of your XCS device for SMTP delivery of outbound mail. The procedure depends on the type of internal mail server you use. See the instructions for your particular mail server to route outgoing mail through the WatchGuard XCS.

The following instructions are for a Microsoft® Exchange mail server.

Exchange 2000 and 2003

For Exchange 2000 and 2003 systems, use the following procedure to add the WatchGuard XCS to the outbound configuration:

1. Open Exchange System Manager.
2. Select **Connectors**.
3. Go to the **Internet Mail SMTP Connector**.
4. Select the **Forward all mail through this connector to the following smart hosts:** option.
5. Type the IP address of your WatchGuard XCS system in square brackets, such as: `[10.0.1.25]`
   To add multiple systems, separate them with commas such as: `[10.0.1.25],[10.0.2.25]`
6. Click **OK**.

Multiple Exchange server configuration

In an environment with multiple Microsoft Exchange servers (not in a clustered configuration), each system must be configured to route outbound mail through the WatchGuard XCS. You can do this on a per-server basis with the SMTP connector configuration on each server, as in the case of single Exchange server environments.

The outbound mail routing configuration can be more efficiently configured by adding an *SMTP Connector* to the **Exchange Routing Groups** configuration rather than the **Servers** configuration item. This Routing Group configuration applies to all your Exchange servers.

To configure the SMTP Connector in a Routing group of Exchange Servers:

1. Open the Exchange System Manager.
2. Select **Routing Groups**.
3. Select the **First Routing Group**.
4. Select **Add**.
5. Select **SMTP Connector**.
6. Type a name for the SMTP Connector, such as `XCSConnector`.
7. Select the **Forward all mail through this connector to the following smart hosts:** option.
8. Type the IP address of your WatchGuard XCS system in square brackets, such as: `[10.0.1.25]`
   To add multiple systems, separate them with commas such as: `[10.0.1.25],[10.0.2.25]`
9. Click **Add** in the **Local bridgeheads** section.
10. Add each Exchange server to the list that must send mail via the WatchGuard XCS.
    Make sure you add all servers and not just the primary Bridgehead server.
11. Select the **Address Space** configuration tab.
12. Use the default values of **Type: SMTP**, **Address: ***, and **Cost: 1**.
13. Click **OK** to save the connector configuration.

Exchange 2007

For Exchange 20007 systems, use this procedure to add the WatchGuard XCS to the outbound configuration:

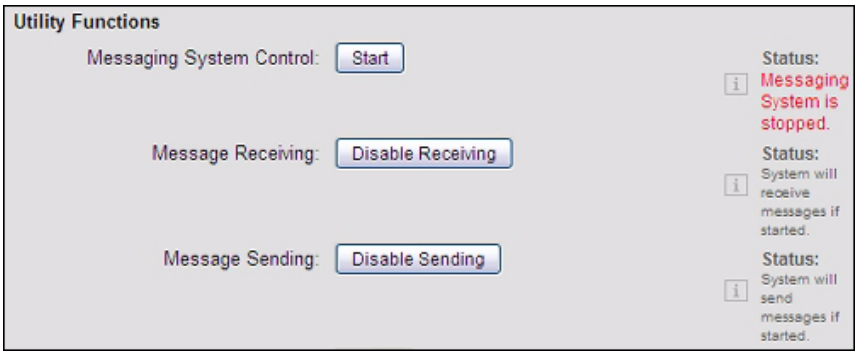
1. Open the Exchange Management Console.
2. Expand the **Organization Configuration** option.
3. Select **Hub Transport**.
4. Select the **Send Connectors** tab.
5. Right-click on the existing **Send Connector**.
6. Select **Properties**.
7. Go to the **Network** tab.
8. Select **Route mail through the following smart hosts:**.
9. Click **Add**.
10. Type the IP address of the WatchGuard XCS system to forward outbound mail to, such as: `10.0.1.25`
    Repeat this procedure to add the addresses of all of your WatchGuard XCS systems.
11. Click **OK**.

Start Message Processing

When the system is configured with your required networking information and mail routes, you can start the messaging system and start to process messages.

To start the messaging system:

1. Select **Activity > Status > Status & Utility**.
2. In the Messaging System Control section, click **Start**.
   The status changes from "Messaging System is stopped" to "Messaging System is running".



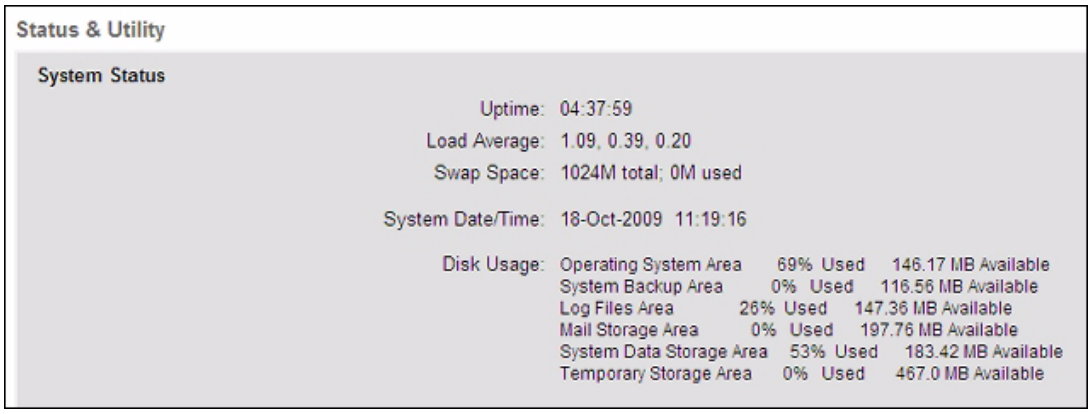
Status and Utility page

The *Status & Utility* page (**Activity > Status > Status & Utility**) provides the following information:

- A snapshot of the system status, including information on uptime, load average, amount of swap space, current date and time, disk usage, RAID status, NTP status, and Anti-Virus pattern file status
- Controls to start and stop the message processing and flush the message queues
- Diagnostic tools, such as a Hostname Lookup function, SMTP Probe, Ping, and Traceroute utilities, that are useful to correct message and networking problems
- System hardware configuration information

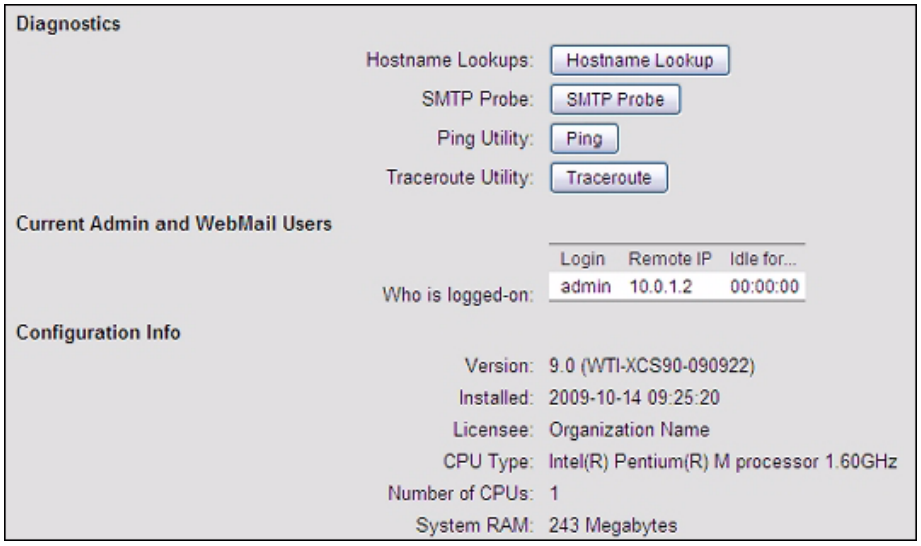
System status

The *System Status* section contains system statistics, such as the total system uptime, load average, the amount of used swap and disk partition space, RAID status, NTP server status, and Anti-Virus pattern update status.


Status & Utility
System Status
Uptime: 04:37:59
Load Average: 1.09, 0.39, 0.20
Swap Space: 1024M total; 0M used
System Date/Time: 18-Oct-2009 11:19:16
Disk Usage: Operating System Area 69% Used 146.17 MB Available
System Backup Area 0% Used 116.56 MB Available
Log Files Area 26% Used 147.36 MB Available
Mail Storage Area 0% Used 197.76 MB Available
System Data Storage Area 53% Used 183.42 MB Available
Temporary Storage Area 0% Used 467.0 MB Available

Diagnostics

The *Diagnostics* section contains networking and SMTP utilities to help troubleshoot network and message delivery issues.



- **Hostname Lookup** —Look up a host on a DNS name server to verify hostname resolution.
- **SMTP Probe** — Send a test email to a remote SMTP server.
- **Ping** — Verify network connectivity with ICMP ping.
- **Traceroute** — Trace the routes of network data from the source to the destination server to verify routing connectivity.

Current admin and WebMail users

Use the *Current Admin and WebMail Users* section to see who is logged in to the web admin interface or through a WebMail session.

Configuration information

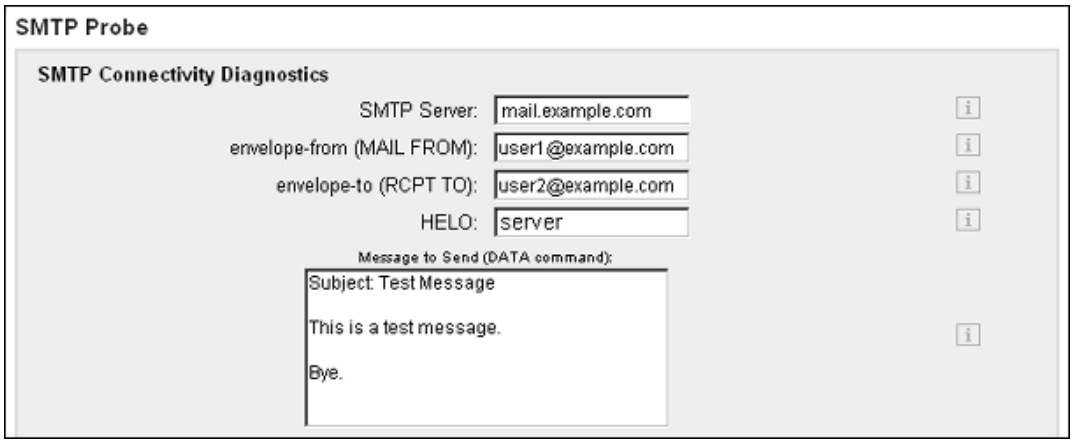
The *Configuration Info* section shows you important system information,such as the current version of the system software, the time it was installed, and license and hardware information.

Testing email connectivity with SMTP probe

The SMTP (Simple Mail Transport Protocol) Probe is used to test email connectivity with a remote SMTP server. With this tool, you can verify that an SMTP server responds to connection requests and returns a valid response.

To do an SMTP probe:

1. In the **SMTP Server** field, type the domain name or IP address of the destination SMTP server that you want to test, such as your internal mail server.



2. Type the **envelope-from (MAIL FROM)** address to identify the sender of the email message.
3. Type the **envelope-to (RCPT TO)** address to identify the recipient of the email message.
4. Type the **HELO** parameter that is used to identify the SMTP Client to the SMTP Server.
   You can enter any value here, but the sending domain name of the server is usually specified.
5. In the **Message to Send (DATA command)** field, type the text to include in the test email message.
   You can enter an optional subject to make sure a blank subject field is not sent.

6. Click **Send Message** to send the test message to the destination SMTP server.

   The response field displays the result of the SMTP diagnostic probe, including the response for each SMTP command sent:

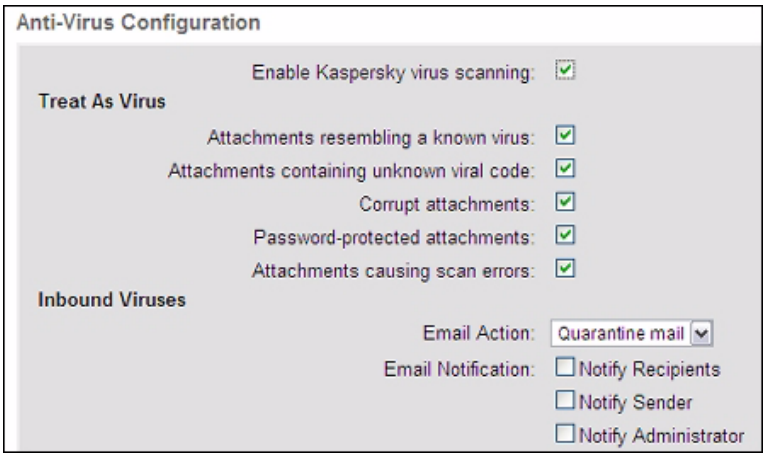
```
Sending mail...
<<< 220 ESMTP Postfix (2.1.0)
HELO example.com
<<< 250 mail.example.com
MAIL FROM:user1@example.com
<<< 250 Ok
RCPT TO:user2@example.com
<<< 250 Ok
DATA
<<< 354 End data with <CR><LF>.<CR><LF>
sending /tmp/smtpdata
.
<<< 250 Ok: queued as F130F33EA6
QUIT
<<< 221 Bye
```

6 Anti-Virus

Anti-Virus Scanning

The virus scanning feature scans all messages (inbound and outbound) that pass through the XCS system for viruses. The WatchGuard XCS integrates the Kaspersky Anti-Virus engine, which is one of the highest rated virus scanning technologies in the world. Virus scanning is tightly integrated with the message processing engine for maximum efficiency.

1. Select **Security > Anti-Virus > Anti-Virus**.



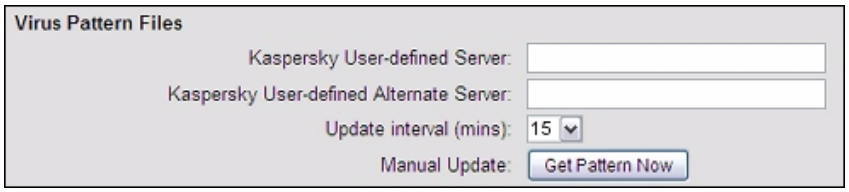
2. Select the **Enable Kaspersky virus scanning** option.
3. Select any additional options in the **Treat As Virus** section.
4. Disable the **Password-protected attachments** option if you do not want attachments with passwords to be considered a virus.
5. Select the **Email Action** to perform for both inbound and outbound mail.

   We recommend you set the inbound action to **Discard** or **Reject mail**. This automatically rejects virus-infected messages instead of storing them in your quarantine. Use **Discard** to discard the message without notification to the sending system. **Reject mail** will send a notification to the sending system which could be a forged sender.

   For outbound mail, set the action to **Quarantine mail** and enable the administrator notification so that you can more easily track the details of an internal virus outbreak.

- **Just log** — Send a log message for the event and take no further action.
- **Reject mail** — Reject the message with notification to the sending system.
- **Quarantine mail** — Put the message in the administrative quarantine area. This is the default action.
- **Discard mail** — Discard the message without notification to the sending system.

6. Select the notifications you want to send when a virus is detected in a message, including the Sender, Recipient, and Administrator.
7. Customize the inbound and outbound notification text as required.
8. Set the **Update interval** for Anti-Virus pattern file updates to *15* minutes for the fastest updates.



9. Click **Apply**.

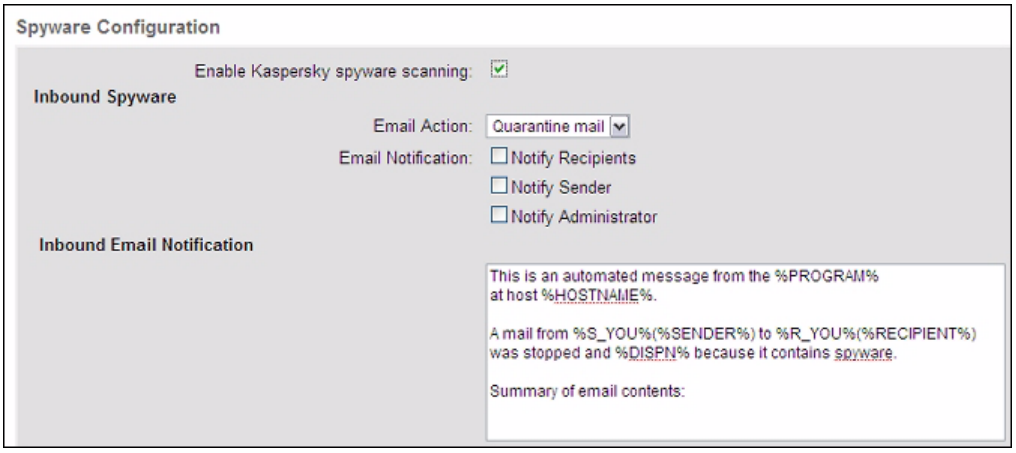
Spyware Detection

The Kaspersky Anti-Virus scanner can detect specific spyware and malware threats, as well as provide Anti-Virus scanning for inbound and outbound email messages and HTTP requests.

The Spyware action is taken after any applicable Anti-Virus action.

To configure Spyware Detection globally:

1. Make sure Kaspersky Anti-Virus is enabled through **Security > Anti-Virus > Anti-Virus**. *Spyware cannot be enabled and configured until Kaspersky Anti-Virus is enabled.*
2. Select **Security > Anti-Virus > Spyware**.


Spyware Configuration
Enable Kaspersky spyware scanning:
Inbound Spyware
Email Action:
Quarantine mail
Email Notification:
Notify Recipients
Notify Sender
Notify Administrator
Inbound Email Notification
This is an automated message from the %PROGRAM% at host %HOSTNAME%.
A mail from %S_YOU%(%SENDER%) to %R_YOU%(%RECIPIENT%) was stopped and %DISPN% because it contains spyware.
Summary of email contents:

3. Select the **Enable Kaspersky spyware scanning** check box.

4. Configure the spyware **Action** to take for both inbound and outbound mail messages.
   This action occurs after any Anti-Virus actions.

   We recommend you set the inbound action to **Discard** or **Reject mail**. This automatically rejects spyware-infected messages instead of storing them in your quarantine. Use **Discard** to discard the message without notification to the sending system. **Reject mail** will send a notification to the sending system which could be a forged sender.

   For outbound mail, set the action to **Quarantine mail** and enable the administrator notification so that you can more easily track the details of an internal spyware outbreak.

   - **Just log** — Send a log message for the event and take no further action.
   - **Reject mail** — Reject the message with notification to the sending system.
   - **Quarantine mail** — Put the message in the administrative quarantine area. This is the default action.
   - **Discard mail** — Discard the message without notification to the sending system.
5. Select the notifications you want to send when a virus is detected in a message, including notifications to the Sender, Recipient, and Administrator.
6. The inbound notification and outbound notification text can be customized as required.

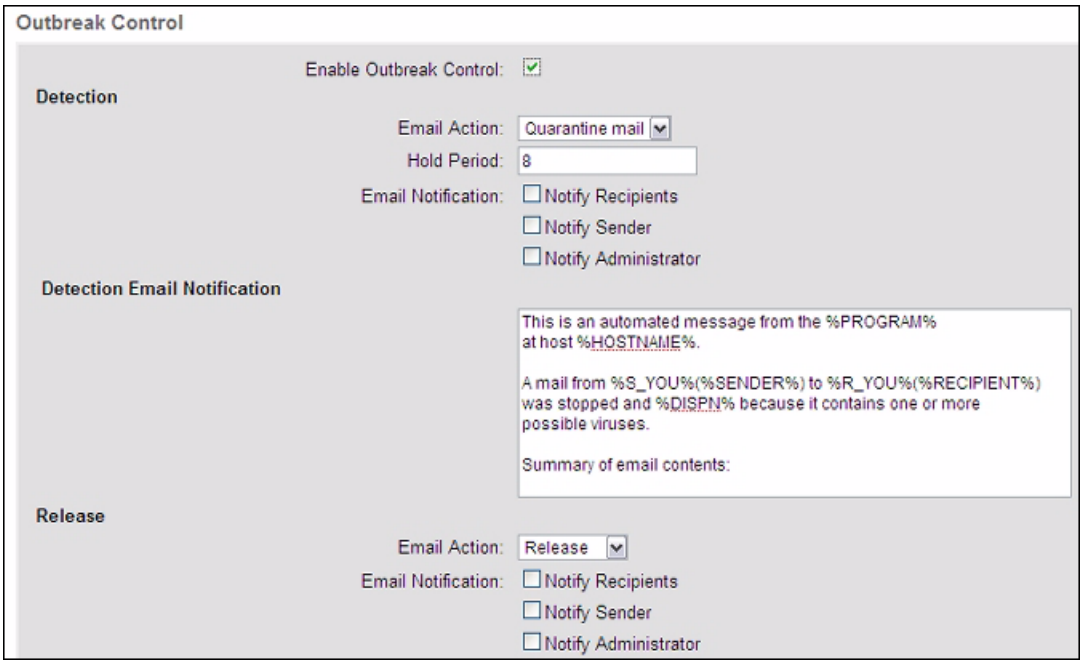
Outbreak Control

The Outbreak Control feature provides customers with zero-day protection against early virus outbreaks. For most virus attacks, the time from the moment the virus is released to the time a pattern file is available to protect against the virus can be several hours.

Outbreak Control can detect and take action against early virus outbreaks to contain the virus threat. If a message contains a possible virus, the message can be quarantined, deleted, or a log message can be sent. When an updated Anti-Virus pattern file is received, any quarantined files are scanned again automatically. If a virus is detected with the new pattern file, the configured Anti-Virus action is taken on the message. If the hold period for a message in the quarantine expires and the message has not been positively identified as a virus in that time, the configured "release" action is taken.

To configure Outbreak Control:

1. Select **Security > Anti-Virus > Outbreak Control**.



2. Select the **Email Action** to take if a message is detected to have a possible virus:
   We recommend to set this action to **Quarantine mail**. This is the default setting.
   - **Just Log** — Deliver the message and send a log message to the log file.
   - **Reject mail** — Reject the message with notification to the sender.
   - **Quarantine mail** — Put the message in the administrative quarantine area. This is the default action.
   - **Discard mail** — Discard the message without notification to the sender.
3. Enter the **Hold Period** (in hours) for which to hold the message in the administrative quarantine area. The default hold period is 8 hours.
4. Select the users who you want to receive a **Notification** if a message is detected as having a possible virus, including the Recipients, the Sender, and the Administrator.
5. Type the text for the automated **Notification Message**.
6. Select the **Action** to take if the **Hold Period** has elapsed for a quarantined message:

- **Just Notify** — Send a message to notify the specified users that the **Hold Period** for a quarantined message has elapsed without it being classified as a virus. The message remains in the quarantine until released manually by the administrator.
- **Release mail** — The message is automatically released from the quarantine and delivered to the original recipients. Notifications can also be enabled to notify users when the message is released. If the message was discarded or rejected by Attachment Control or Malformed Mail and was then quarantined by Outbreak Control, the message is discarded on release. The final action is Outbreak Control and Quarantine because of a possible virus.

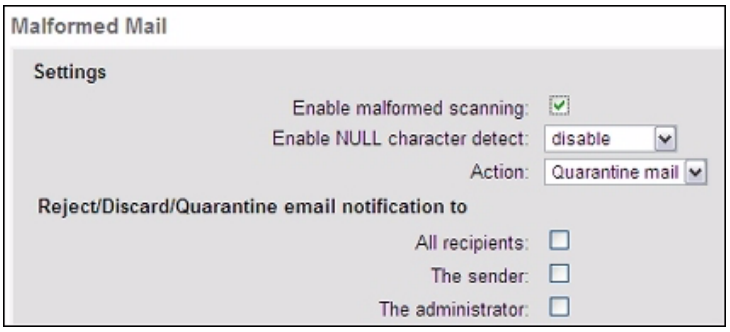
7. Select the users you want to receive a **Notification** if a message is released from the quarantine, including the Recipients, the Sender, and the Administrator.
8. Type the text for the automated **Notification Message**.
9. Click **Apply**.

Malformed Mail

Many viruses and denial of service (DoS) attacks conceal themselves in malformed messages to try to elude virus scanners. The scan engines cannot detect the attachment and therefore pass the complete message through to an internal server. Some mail clients try to rebuild malformed messages and may rebuild or activate a virus-infected attachment. Other types of malformed messages are designed to attack mail servers directly. Most often these types of messages are used in denial-of-service (DoS) attacks.

To configure malformed mail scanning:

1. Select **Security > Anti-Virus > Malformed Mail**.



2. Select the **Malformed Scanning** check box.
3. Make sure **Enable NULL character detect** is set to **Disable**.

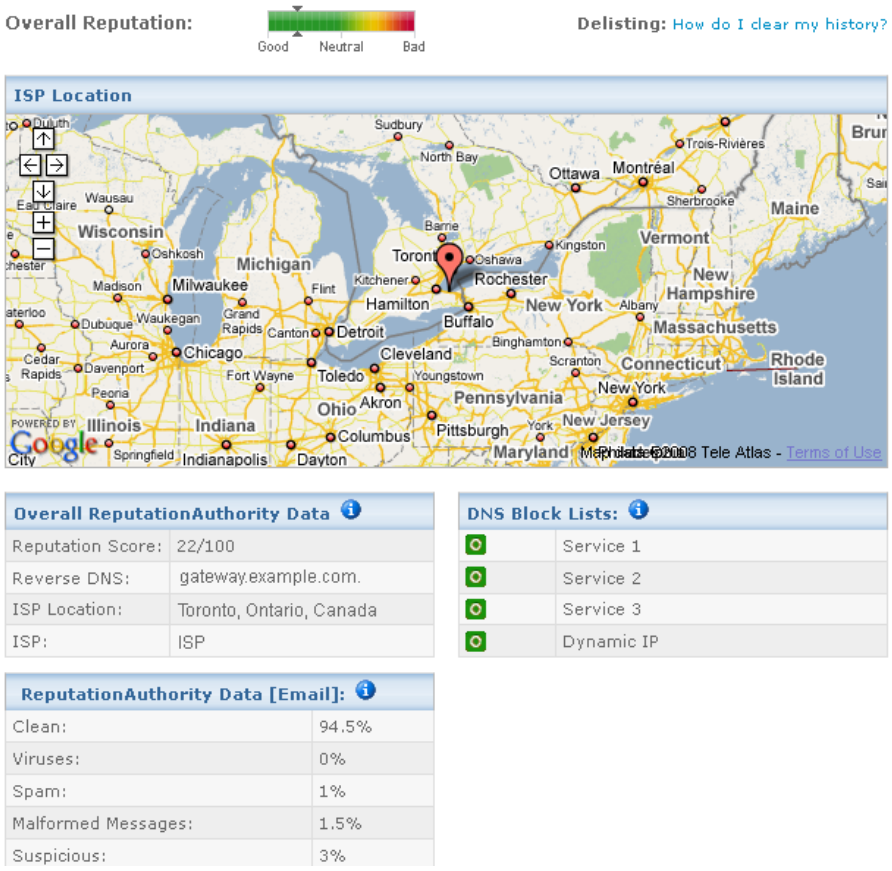
   A null character is a character in the raw mail body of the message that has a byte value of 0. The null character detection feature may cause incompatibility with certain mail servers and it is recommended that this feature be disabled if issues occur.
4. Select an **Action** to take when a malformed message is detected.

   We recommend you set the action to **Quarantine mail**. This is the default setting.
   - **Just log** — Send a log message to the log file and take no further action.
   - **Reject mail** — Reject the message with notification to the sending system.
   - **Quarantine mail** — Put the message in the administrative quarantine area. This is the default action.
   - **Discard mail** — Discard the message without notification to the sending system.
5. Click **Apply**.

7 ReputationAuthority

ReputationAuthority

The ReputationAuthority helps to identify spam. It reports behavior information for a collection of metrics about the sender of a mail message, based on information collected from installed products and global DNS Block Lists. The metrics it reports include the sender's overall reputation, whether the sender is a dial-up, and whether the sender appears to be virus-infected or sends large amounts of spam messages.

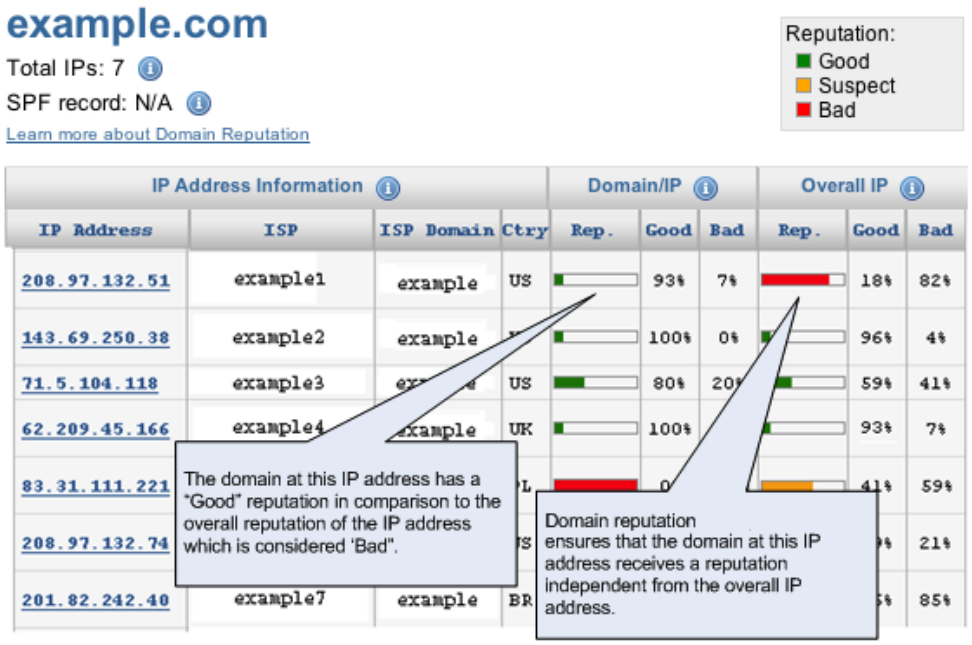


This information can be used by the WatchGuard XCS to either reject the message immediately or contribute to the Intercept score if a message is detected from a source with a poor reputation or numerous virus infections.

If the ReputationAuthority option is enabled, the system queries for statistics from the ReputationAuthority service for the sender IP address of each message received, excluding those from trusted and known networks. With the information returned from ReputationAuthority, the system can make a decision about whether a message is spam or legitimate email. A reputation of "0" indicates the sender is extremely reliable and rarely sends spam or viruses. A reputation of "100" indicates the sender is extremely unreliable and often sends spam or viruses. An IP address with no previous information from any source is assigned a value "50".

Domain and sender reputation

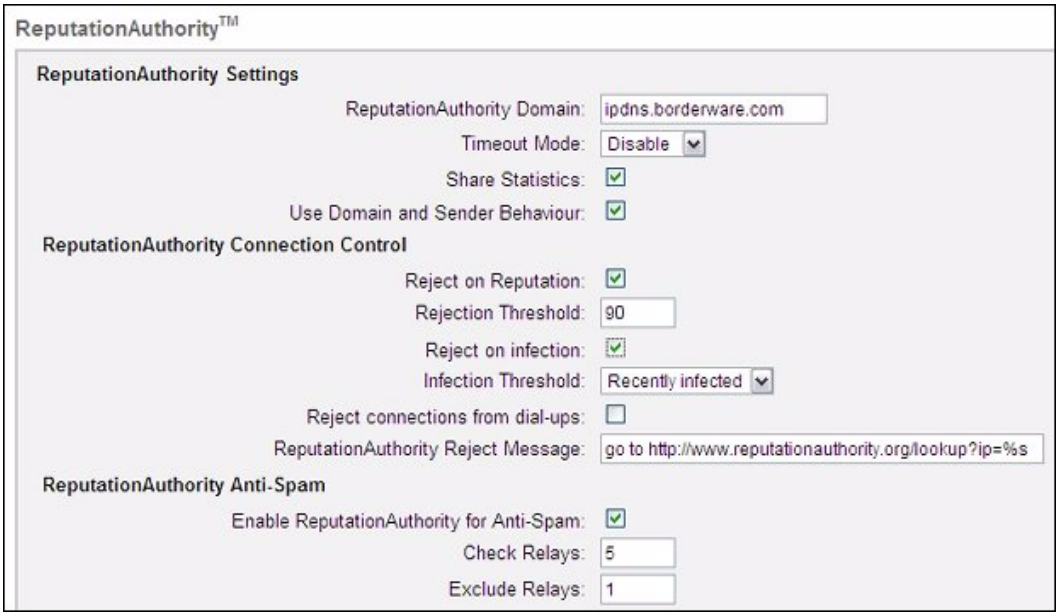
Domain and Sender Reputation increases the reputation effectiveness by examining not only the IP reputation of a sender, but also the domain name and envelope sender information from that IP address. A domain can receive a reputation independent of the behavior of another domain originating from the same address. A specific sender address can receive a reputation independent of the behavior of another sender address from the same domain or IP address. For a message from the sender user@example.com, a query will be sent to ReputationAuthority checking the sender address user@example.com, the domain example.com, and the originating IP address of the connection.



Configure ReputationAuthority checks

To configure ReputationAuthority:

1. Select **Security > Anti-Spam > ReputationAuthority**.



2. Enter the ReputationAuthority **Domain** to query.
   The default domain is WatchGuard's Reputation domain. We recommend you do not edit this domain.
3. Select the **Share Statistics** check box to allow ReputationAuthority information, such as spam and virus statistics for connecting client IP addresses, from this system to be shared with the ReputationAuthority network.

   You must enable TCP port 443 outbound to allow statistics to be uploaded to the Reputation Server. There are no security risks associated with sharing statistics. The system does not relay any private or sensitive information to the ReputationAuthority.

4. Select the **Use Domain and Sender Behaviour** check box to make use of domain and sender behavior when the system performs ReputationAuthority queries.
   This option increases the effectiveness of ReputationAuthority. *When this option is selected, the XCS examines not only the IP reputation of a sender, but also the domain name and envelope sender information from that IP address.*
5. Select the **Reject on Reputation** check box to reject messages from senders whose reputation is above the configured **Reputation Threshold**.

   A reputation of "0" indicates the sender is extremely reliable and rarely sends spam or viruses. A reputation of "100" indicates the sender is extremely unreliable and often sends spam or viruses. An IP address with no previous information from any source is assigned a value "50".

   To override a ReputationAuthority reject, add the system to the internal hosts and friendly mail relays list. You can also override ReputationAuthority rejects if you create a Specific Access Pattern to **Trust** the rejected address. ReputationAuthority rejects cannot be overridden by a policy. Pattern Based Message Filtering can also be set to **Bypass** (to bypass all Anti-Spam and content checks), **Trust** (to accept and train as valid mail) or **Accept** (just accept without training) the message, however, this can interfere with later message processing. We recommend that you use the mail relays list.

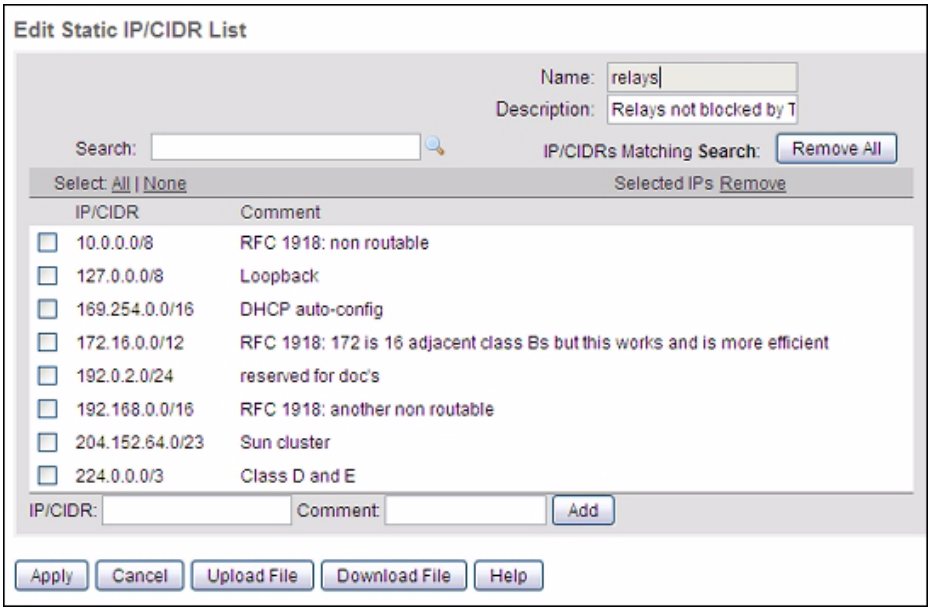
6. Enter a **Rejection Threshold** over which a message is rejected.
   It is recommended to leave the threshold at the default value of "90". The lower the reputation threshold, the greater the chance that a system with valid mail will be blocked. This setting is only valid when **Reject on Reputation** is enabled.
7. Select the **Reject on Infection** check box to reject messages from senders whose infection score is above the configured *Infection Threshold*.
8. Enter an **Infection Threshold** that indicates the criteria for rejecting messages based on whether the sending host is **Currently infected** (received in last hour), or **Recently infected** (received in last day). *This setting is only valid when Reject on Infection is enabled.*
9. We recommend that you keep the **Reject Connection From Dial-ups** option disabled.
10. Customize the **ReputationAuthority Reject Message** as required.
11. Select the **Enable ReputationAuthority for Anti-Spam** check box to check incoming messages against the spam information gathered by the ReputationAuthority network. The Reputation score is factored in the overall Intercept Anti-Spam decision for the message.
12. Click **Apply**.

Trusted clients and known mail servers

Administrators can trust friendly local networks or addresses of known mail servers in their environment that relay mail through this system. These specific networks and servers can be added to the *relays* IP Address list in the Threat Prevention configuration page to make sure these servers are not blocked by Threat Prevention and ReputationAuthority. This also makes sure that reputation statistics for these addresses are not reported to ReputationAuthority.

To add a system to the *relays* list:

1. Click the **internal hosts and friendly mail relays** link on the ReputationAuthority page.
   The relays Static IP/CIDR List screen appears.



2. Add the address of any internal relays, including a descriptive comment.
3. Click **Add**.

8 Anti-Spam

Intercept Anti-Spam Overview

The Intercept Anti-Spam features take advantage of the extensive message control features of the WatchGuard XCS, and provide a solutions-based approach in which each anti-spam component, when enabled, provides input to the final spam score of a message. Information retrieved by all of the enabled Anti-Spam components results in a more informed decision on whether the message is in fact spam or legitimate mail.

Thresholds can be set to take appropriate action on a message based on its score and classification, such as *Certainly Spam*, *Probably Spam*, and *Maybe Spam*. A different action can be set for each threshold, such as "Reject" for messages that are classified as *Certainly Spam*, or "Modify Subject Header" for messages that are classified as *Maybe Spam*.

Administrators can use the advanced Intercept options to provide more granular control over each Anti-Spam Intercept component for their environment; however, the default Intercept configuration has been engineered to provide maximum protection against spam without additional configuration.

The Intercept Anti-Spam engine includes the following components:

Spam Words
: Filters messages based on a dictionary of typical spam words and phrases that are matched against the message.

Mail Anomalies
: Checks various aspects of the incoming message for issues such as unauthorized SMTP pipelining, missing headers, and mismatched identification fields.

DNS Block List (DNSBL)
: Detects spam using domain-based lists of hosts that have a poor reputation. Messages can also be rejected immediately, regardless of the results of other Anti-Spam processing, if the client appears on a DNSBL. A configurable threshold allows administrators to specify how many DNSBLs must be triggered to consider the sender as unreliable.

URL Block List
: URL Block Lists contain a list of domains and IP addresses of URLs that have appeared previously in spam messages. This feature is used to determine if the message is spam by examining any URLs contained in the body of a message to see if they appear on a block list.

ReputationAuthority
The ReputationAuthority helps to identify spam by reporting a collection of metrics about the sender of a mail message, including their overall reputation, whether the sender is a dial-up, and whether the sender appears to be virus-infected, based on information collected from installed WatchGuard XCS products and global DNS Block Lists. This information can be used by Intercept to reject the message, or be used as part of the overall anti-spam decision.

Token Analysis
Detects spam based on advanced content analysis against databases of known spam and valid mail.

Backscatter Detection
Detects spam based on signature verification of the Envelope Sender to prevent spam bounce emails to forged sender addresses.

Sender Policy Framework (SPF)
Performs a verification of a sending host's SPF DNS records to identify and validate the source of a message to determine whether a message was spoofed.

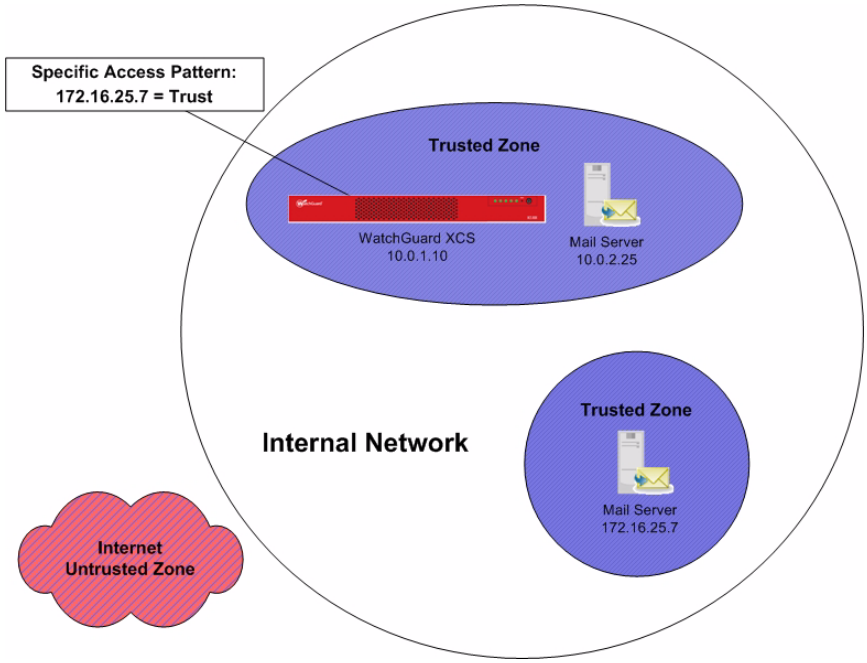
DomainKeys Authentication
Performs a check of a sending host's DomainKeys DNS records to identify and validate the source of a message to determine whether a message was spoofed.

Trusted and untrusted mail sources

The WatchGuard XCS must be correctly configured for interaction with local and remote mail servers. The system only processes mail through the spam filters when a message originates from an untrusted source. Mail from trusted sources bypass the spam controls.

There are two ways to control how sources of mail are identified and trusted:

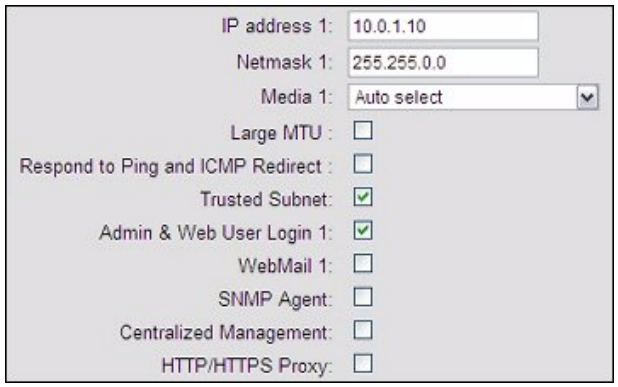
- **Trusted Subnet** — All mail from a specific network interface is considered trusted.
- **Specific Access Pattern** — An IP address (or address block), server, or domain name is identified as trusted through a specific access pattern rule.



Trusted subnet

To specify a network interface as trusted or untrusted:

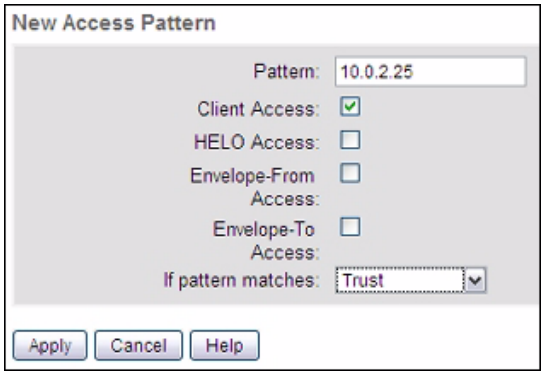
1. Select **Configuration > Network > Interfaces**.
2. For the specified interface, enable or disable the **Trusted Subnet** check box.
   The Trusted Subnet setting should not be used if the system is deployed internally or behind a network firewall.



Trust through specific access patterns

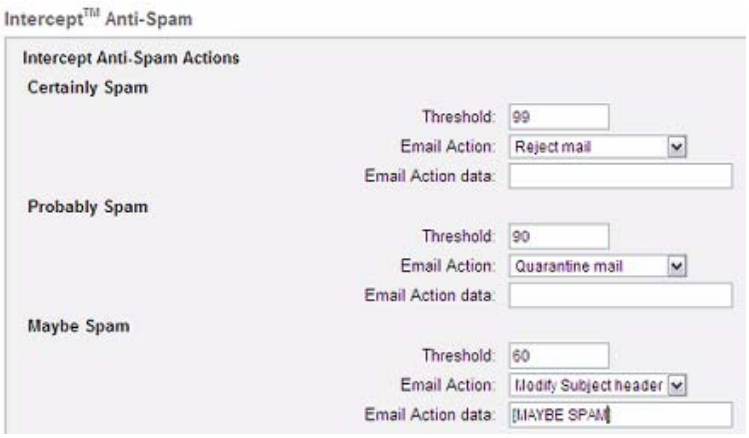
To trust a system with a specific access pattern:

1. Select **Configuration > Mail > Access**.
2. For Specific Access Patterns, click **Add Pattern**.
3. Type the IP address or hostname of the system in the **Pattern** field.
4. Select the **Client Access** check box.
5. From the **If pattern matches** drop-down list, select **Trust**.
6. Click **Apply**.



Configure Intercept Anti-Spam

1. Select **Security > Anti-Spam > Anti-Spam**.



You can assign actions for three levels of spam score thresholds:

Certainly Spam
: Any message with a score over this threshold (Default: 99) is *Certainly Spam*. These types of messages require a strong action such as **Reject Mail** or **Discard Mail**.

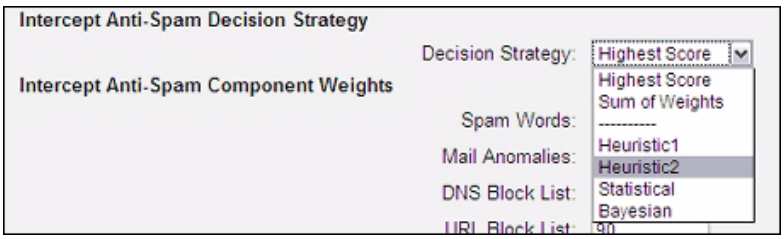
Probably Spam
: Any message with a score over this threshold (Default: 90) is probably spam. This threshold indicates a message with a very high spam score, but not high enough to be *Certainly Spam*. You can treat this messages with a lighter action than *Certainly Spam*, such as **Quarantine Mail**, but we do not recommend that you reject these messages.

Maybe Spam
: Any message with a score over this threshold (Default: 60) could be spam but should be treated with caution to prevent false positives. This threshold indicates messages which could be spam, but could also be legitimate mail. We recommend that an action such as **Modify Subject Header** be used. With this action, the message is delivered to the end user with a modified subject header to alert the user that the message could be spam.

Intercept decision strategy

The Intercept Decision Strategy allows administrators to modify the way in which Intercept processes messages for spam.

We recommend that you choose the **Heuristic 2** decision strategy. **Heuristic 2** is a passive strategy that is effective for most environments and provides an excellent spam catch rate with a very low chance of false positives.



Heuristic 1

Components are divided into objective and subjective categories. Objective components are DNS Block List, URL Block List, Mail Anomalies, ReputationAuthority Dial-up, SPF, and DomainKeys. Subjective components are Spam Words, Token Analysis, and ReputationAuthority reputation. The message is classified initially by a combination of the subjective scores and the classification is then adjusted by combining the objective scores. A baseline is established with a subjective filter. If Token Analysis scores a message at 60, a baseline of *Maybe Spam* is established. If one additional objective filter triggers, the message is categorized as *Probably Spam*. Two objective filters increase the level to *Certainly Spam*.

Heuristic 2

This strategy is similar to the **Heuristic 1** strategy except that the subjective component scores are weighted more heavily in the final decision than in Heuristic1. In environments where there is no Token Analysis training on outbound legitimate mail (such as some evaluation scenarios), or for new installations, **Heuristic 2** can result in an increase in false positives. In this case, administrators can use the Heuristic 1 strategy, which is identical to **Heuristic 2** except that Token Analysis is de-emphasized and additional Anti-Spam features must be triggered for a message to be considered *Probably Spam* or *Certainly Spam*. When you use Intercept for the first time, we recommend that **Heuristic 1** be used until a suitable amount of training has been accumulated, and then you can change to **Heuristic 2**.

See the **User Guide** for more detailed explanations of the different Intercept Anti-Spam decision strategies.

9 Directory Services

Directory Services

The WatchGuard XCS can use *LDAP (Lightweight Directory Access Protocol)* services to get access to directories (such as Active Directory, OpenLDAP, and iPlanet) for user and group information.

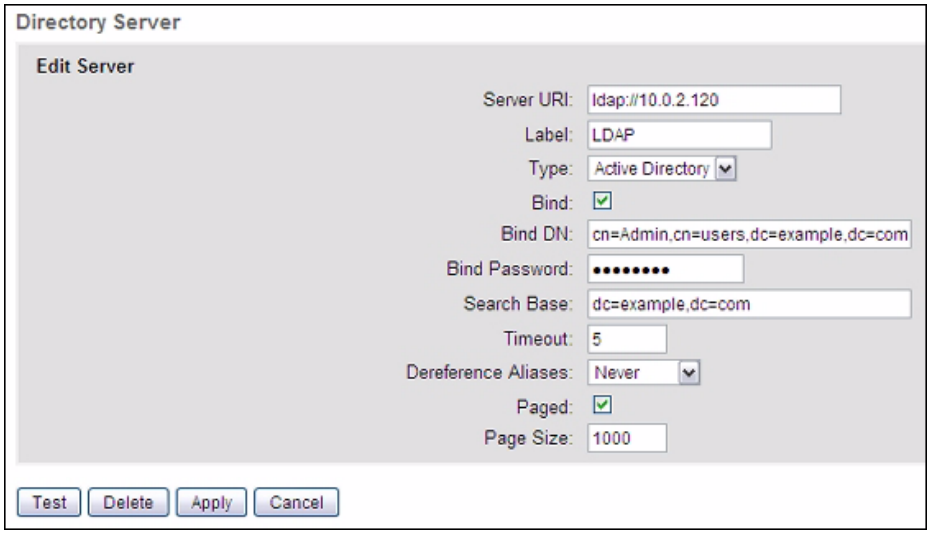
You can use LDAP for these tasks:

- User and group membership lookups for policies
- User lookups for Reject on Unknown Recipient feature
- Alias and virtual mappings
- Remote authentication
- Mail routing

Directory servers

To configure directory servers:

1. Select **Configuration > LDAP > Directory Servers**.
2. Click **Add** to configure a new directory server, or click **Edit** to modify an existing server.



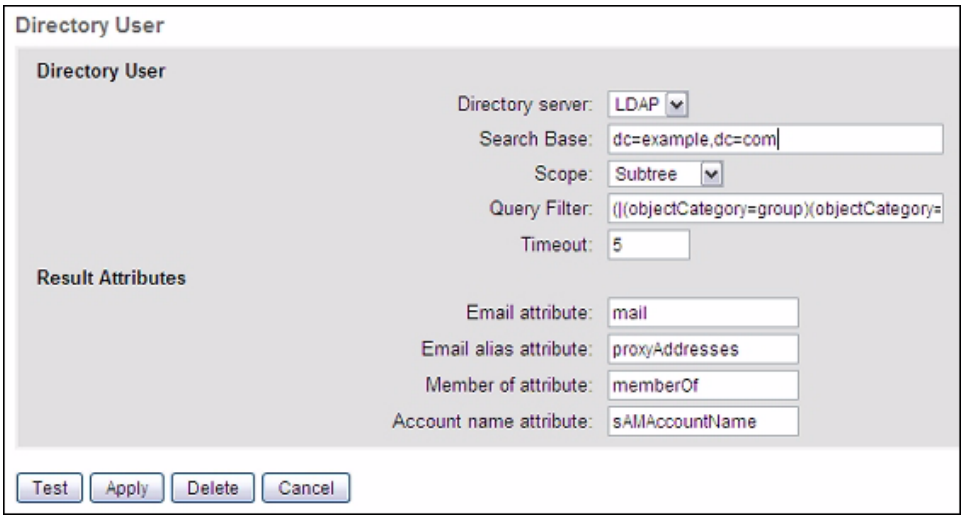
3. Type the **Server URI** (Uniform Resource Identifier) address, such as `ldap://10.0.2.120`.
   To query an Active Directory global catalog, add the port number 3268 to the server URI, such as ldap://10.0.2.120:3268. Use "ldaps:" if you use SSL with the LDAP server directory.
4. Type an optional **Label** or alias for the LDAP server.
5. Select the **Type** of LDAP server you use, such as **Active Directory**, or choose **Others** for OpenLDAP or iPlanet.
6. Select the **Bind** check box.
7. Type the **Bind DN** (Distinguished Name). For example, for Active Directory, use:
   `cn=Administrator,cn=users,dc=example,dc=com`
   Older Windows login names, such as `DOMAIN/Administrator`, are also supported. Make sure that you enter a bind DN specific to your environment. In Active Directory, if you use an account other than Administrator to bind to the LDAP server, the name must be specified as the full name, not the account name. For example, use “John Smith” instead of “jsmith”.
8. Type the **Bind Password** for the LDAP server.
9. Specify a default **Search Base** for lookups. For example: `dc=example,dc=com`.
10. Type the maximum **Timeout** interval, in seconds, to wait for the search to complete.
    Valid values are from 1 to 100 seconds.
11. Use the **Dereference Aliases** option to set how alias dereferences are performed during a search:
    - **Never** — Aliases are never dereferenced.
    - **Searching** — Aliases are dereferenced in subordinates of the base object, but not in locating the base object of the search.
    - **Finding** — Aliases are only dereferenced when locating the base object of the search.
    - **Always** — Aliases are dereferenced when searching and locating the base object of the search.
12. Select the **Paged** check box to enable paging support for an Active Directory server.
    When queries are sent to an LDAP server, the amount of information returned can contain thousands of entries and sub-entries. When you select the Paged check box, LDAP information is retrieved in more manageable sections to control the rate of data return.
13. Enter the **Page Size** for an Active Directory server.
    If this field is left blank, the default value of 1000 is used. The Page Size must match the size configured in the Active Directory server's LDAP query policy.
14. Click **Apply**.

Directory users

You can use the *Directory Users* feature to import user account and group membership data from LDAP-based directory servers.

To configure directory users:

1. Select **Configuration > LDAP > Directory Users**.
2. Click **Add**.



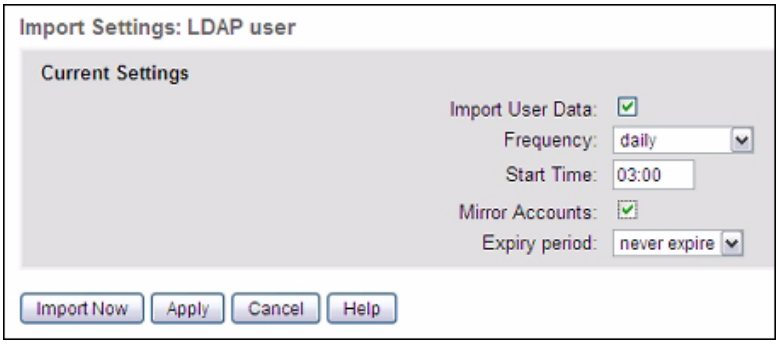
3. Select a **Directory Server** to perform the search.
4. Type the **Search Base** to start the search from. For example: `dc=example,dc=com`.
5. Type the **Scope** of the search.
   - **Base** — Searches the base object only.
   - **One Level** — Searches objects beneath the base object, but excludes the base object.
   - **Subtree** — Searches the entire subtree, of which the base distinguished name is the topmost object, including that base object.
6. Type the appropriate **Query Filter**. For example, for Active Directory use:
   `(|(|(objectCategory=group)(objectCategory=person))(objectCategory=publicFolder))`
   This query filter includes mail-enabled Exchange public folders to prevent them from being rejected if *Reject on Unknown Recipient* is enabled. For iPlanet and OpenLDAP, use the `(objectClass=person)` query filter.
7. Type the maximum **Timeout** interval, in seconds, to wait for the search to complete.
   Valid values are from 1 to 100 seconds.
8. Type the **Email attribute** that identifies the user's email address.
   For Active Directory, iPlanet, and OpenLDAP, use "mail".
9. Type the **Email alias attribute** that identifies the user's alternate email addresses.
   In Active Directory, the default is proxyAddresses. For iPlanet, use Email. For OpenLDAP, leave this field blank.
10. Type the **Member Of** attribute that identifies the group(s) that the user belongs to.
    This information is used for Policy controls. In Active Directory, the default is memberOf. For iPlanet, use Member. For OpenLDAP, leave this field blank.
11. Type the **Account Name Attribute** that identifies a user's account name for login.
    In Active Directory, the default is sAMAccountName. For iPlanet, use uid. For OpenLDAP, use cn.
12. Click **Test** to test your LDAP settings.
13. Click **Apply**.

Import settings

The system can automatically import LDAP user data on a scheduled basis to stay synchronized with the LDAP directory.

To import LDAP users and groups:

1. Select **Configuration > LDAP > Directory Users**.
2. Click **Import Settings**.



3. Select the **Import User Data** check box to enable automatic import of LDAP user data.
   This helps to make sure that your imported LDAP data remains current with the information on the LDAP directory server.
4. Select the **Frequency** of LDAP imports.
5. Specify the **Start Time** for the import in the format hh:mm. For example, to schedule an import at midnight enter `00:00`.
6. Click **Apply**.
7. Click **Import Now** to immediately start the import of users.
   *You can see the progress of LDAP imports at **Activity > Logs > System**.*

Mirror LDAP accounts as local users

Administrators can mirror existing LDAP accounts, which creates a locally-stored account on the WatchGuard XCS for each imported user. If you have enabled the Spam Quarantine feature and the Trusted/Blocked Senders lists, this provides a simple method to allow directory-based users to view and manage quarantined messages

1. Select the **Mirror accounts** check box.
2. Choose an **Expiry period** for the mirrored accounts.
   If the user no longer exists in the LDAP directory for the specified period of time, the local mirrored account is deleted. This option only applies to a local mirrored account and does not apply to accounts used for the Reject on Unknown Recipients feature.
3. Click **Apply**.
4. Click **Import Now** to immediately start the import of users and create mirrored accounts.
   *You can see the progress of LDAP imports at **Activity > Logs > System**. You can see mirrored accounts at **Administration > Accounts > Mirrored Accounts**.*

10 Content Control

Attachment Control

Attachment filters can be used to control a wide range of problems caused by both inbound and outbound attachments in email messages and web requests.

- **Viruses and Spyware** — Attachments and downloads that carry viruses, spyware, and other types of malware can be blocked.
- **Offensive Content** — The system blocks the transfer of images, which reduces the possibility that an offensive picture will be transmitted to or from your company messaging and web systems.
- **Confidentiality** — Prevents the transmission of unauthorized documents through the system.
- **Loss of Productivity** — Prevents your systems employee abuse.

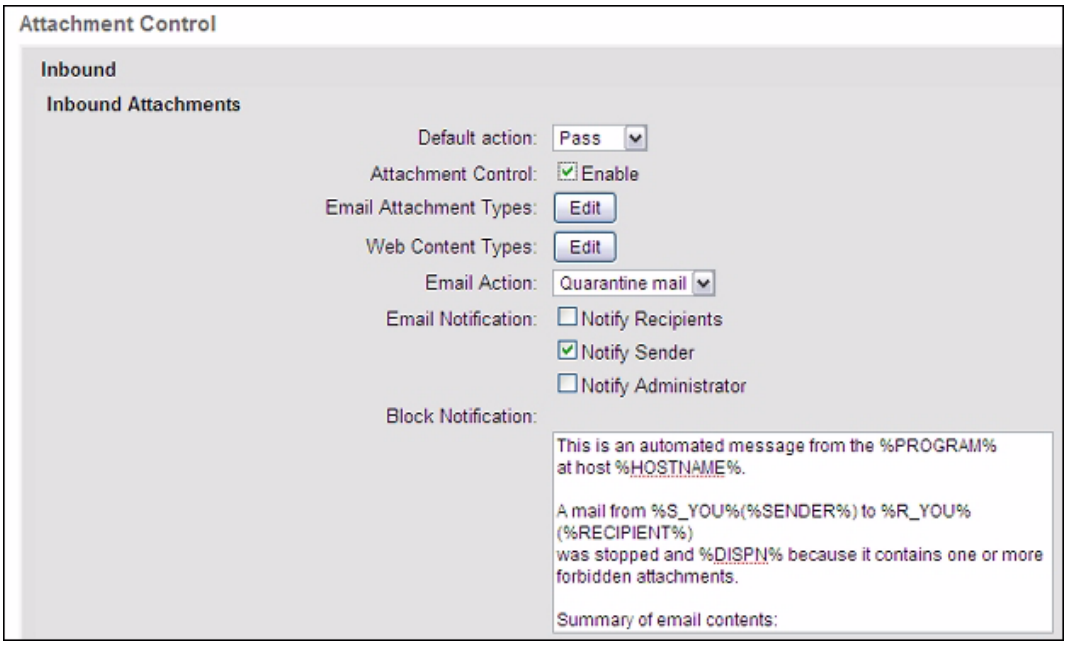
Attachment controls are based on the following characteristics:

- **File Extension Suffix** — The suffix of the file is checked to determine the attachment type, such as .exe, or .jpg.
- **MIME Content Type** — MIME (Multipurpose Internet Mail Extensions) can be used to identify the actual content type of the message.
- **Content Analysis** — The file is analyzed to look for characteristics that can identify the file type. This analysis makes sures that the attachment controls are not circumvented, for example, by a simple file rename.

Configure Attachment Control

To configure Attachment Control:

1. Select **Security > Content Control > Attachment Control**.



2. Select the **Default Action** ("Pass" or "BLOCK") for attachment control for items not specifically shown in the *Attachment Types* list or attachments that cannot be identified.

   The default is "Pass", which allows all attachments. Any file types defined in the Attachment Types list overrides the default setting.
3. Select the **Attachment Control** check box.
   This option can be set for both inbound and outbound messages.
4. Click **Edit** to configure the action for **Email Attachment Types**.
   You can also configure separate actions for web content types.
5. Select an **Action** to perform if attachment control blocks an email attachment.

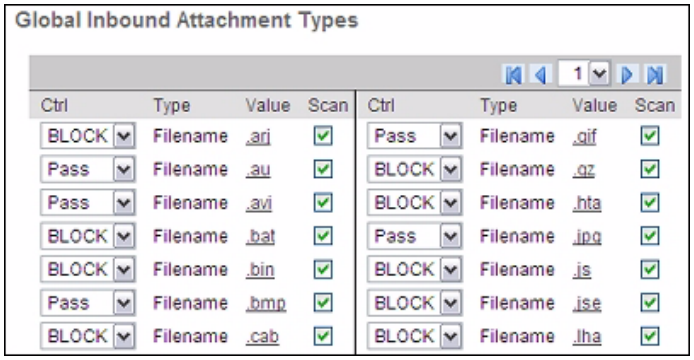
   We recommend that you set this action to **Quarantine Mail**. This is the default setting.
   - **Just log** — Log the event and take no further action.
   - **Reject mail** — The message is rejected and a notification is sent to the sending system.
   - **Quarantine mail** — The message is placed into the administrative quarantine area. This is the default action.
   - **Discard mail** — The message is discarded without a notification to the sending system.
6. Enable and customize **Notifications** for inbound and outbound messages.
   Notifications are not sent for "Just Log" actions.
7. Customize the **Stripped Attachment Text** that will replace stripped attachments.

   This text can be customized for both inbound and outbound messages. The replacement text attachment uses the content type of "text/plain" and uses the character set US-ASCII.
8. Click **Apply**.

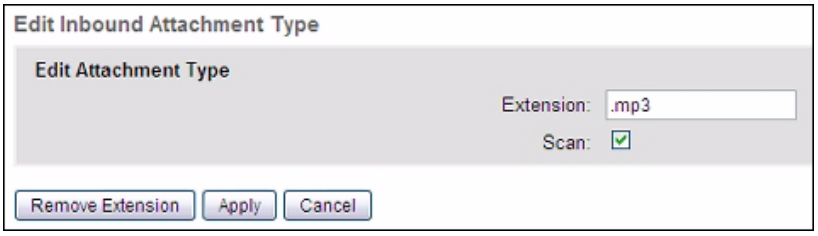
Edit attachment types

To edit attachment types:

1. Click **Edit** to edit your attachment types for email or web content.
   You can add file extensions for email messages (such as .mp3), or MIME content types for both email and web content (such as image/png).


Global Inbound Attachment Types
1
Ctrl Type Value Scan Ctrl Type Value Scan
BLOCK Filename .ari Pass Filename .gif
Pass Filename .au BLOCK Filename .gz
Pass Filename .avi BLOCK Filename .hta
BLOCK Filename .bat Pass Filename .jpg
BLOCK Filename .bin BLOCK Filename .js
Pass Filename .bmp BLOCK Filename .jse
BLOCK Filename .cab BLOCK Filename .lha

2. For each attachment type, choose whether you want to **Pass**, **Strip** (for mail messages only), or **BLOCK** the attachment.
   For attachments with no extension specified, there is a file type called **[no extension]** that is set to a default of **Pass**.
3. Select the **Scan** check box to scan the contents of attachments with the specified extension.
4. Click the **Add Extension**.



   - **Extension** — Type a specific attachment type extension or MIME type, such as `.mp3` or `image/png`. HTTP Web content can only be detected based on MIME types.
   - **Scan** — Select the **Scan** check box to enable scanning for the selected extension or MIME type. The system can scan files within an archive file (such as .zip) for forbidden attachments. If an archive file, such as .zip, contains a file type that is blocked, the archive file is blocked, even if it is set to Pass. Disable the **Scan** option if you do not want to scan the content of the specific archive file type.

You must enable Anti-Virus scanning to allow archive files to be decompressed and checked for forbidden attachments.

5. Click **Apply**.

Attachment stripping

The Attachment Control feature provides the ability to identify and remove attachments from inbound and outbound mail messages. You can configure a list of specific attachment extensions or MIME types to strip from a message before it is delivered. A configurable notification text attachment will replace the attachment that was removed to indicate to the user that the attachment was stripped and specify the reason why it was removed.

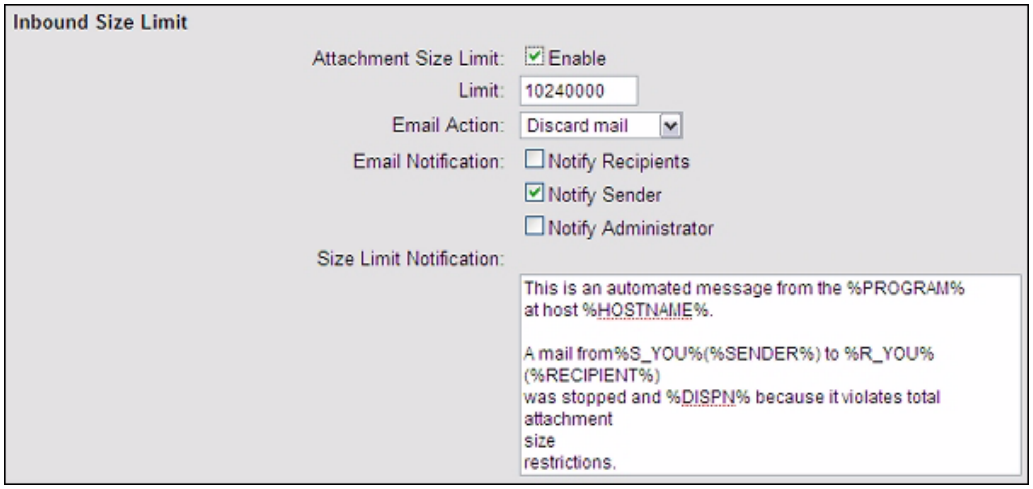
Attachment size limits

The Attachment Control feature can filter inbound and outbound mail messages based on the size of their attachments. Administrators can set a size limit threshold that triggers an action if it is exceeded. If there is more than one attachment to the message, the attachment sizes are added together. Attachment size limits can be set globally and in policies.

Attachment size limits are checked before any other attachment control function, and size limit actions take precedence over attachment control actions.

To configure attachment size limits:

1. Select **Security > Content Control > Attachment Control**.



2. Select the **Attachment Size Limit** check box.
3. Type the attachment size **Limit** (in bytes).

   Attachments greater than this threshold trigger the **Email Action** defined in the next step. The default is 10240000 bytes. Set to 0 to indicate no limit.

   The **Maximum Message Size** configured in **Configuration > Mail > Access** is also set to 10240000 bytes, and this threshold is exceeded if the attachment size is close to the attachment size limit. It is recommended that the **Maximum Message Size** value be at least 1.5 times the value of the **Attachment Size Limit** option to make sure that large attachments do not exceed the **Maximum Message Size**.
4. Select an **Email Action** to take on an email message when the attachment size threshold limit has been exceeded.
   - **Just log** — Send a log message for the event and take no further action.
   - **Reject mail** — Reject the message and send a notification to the sending system.
   - **Quarantine mail** — Put the message in the administrative quarantine area.
   - **Discard mail** — Discard the message without sending a notification to the sending system.
5. Enable and customize **Notifications** for inbound and outbound messages.
   Notifications are not sent for "Just Log" actions.
6. Click **Apply**.

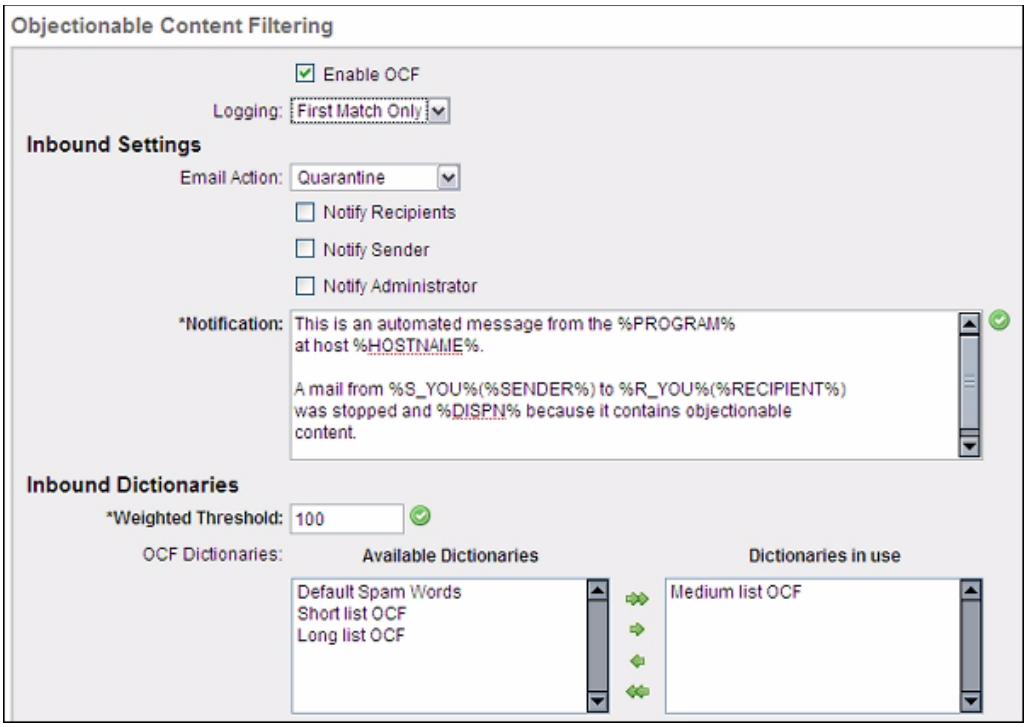
Objectionable Content Filter

The Objectionable Content Filter (OCF) defines a list of key words that cause a message to be blocked if any of those words appear in the message. The Objectionable Content Filter provides enhanced content filtering functionality and flexibility, and allows users to restrict content of any form, including objectionable words or phrases and offensive content.

OCF has a maximum of 35 characters for a word. OCF does not detect plurals of words. Both plural and singular word forms must be defined in the dictionaries.

To configure OCF:

1. Select **Security > Content Control > Objectionable Content**.



2. Select the **Enable OCF** check box.
3. Set the type of **Logging** to perform for OCF processing.
   - **No Logging** — No OCF logging is performed.
   - **First match only** — Send a log message for the first word that was matched by the filter.
   - **All matches** — Send a log message for all words that were matched by the filter.
4. Set the **Action** for both inbound and outbound messages. We recommend you use the **Quarantine mail** action. This is the default setting.
5. If the dictionary is a weighted dictionary, set the **Weighted Threshold** for OCF to consider a message as containing objectionable content. This value must be an integer between 1 and 9999. The default is 100.

   If the aggregate weight of the OCF words found in a message matches or exceeds this threshold, OCF takes the configured action. If both weighted and unweighted dictionaries are used, the final action is triggered if the sum of the weights exceeds the configured weighted threshold, or if a match occurs in an unweighted dictionary.

6. Select the **OCF Dictionaries** to use with inbound and outbound OCF.
   The dictionaries available are shown in the **Available Dictionaries** section. Use the arrow buttons to move the dictionaries to the **Dictionaries in Use** section as required. The default OCF dictionaries consist of a "Short", "Medium", and "Long" list of common objectionable words and phrases. Organizations can create their own OCF dictionary files with the **Security > Content Control > Dictionaries & Lists** feature.

   The OCF dictionaries contain content that is of a vulgar nature. The pre-defined dictionaries should be viewed with caution as they contain words and phrases that may be offensive. All dictionaries should be reviewed and modified as required before you enable them for use with OCF.

7. Enable and customize **Notifications** for inbound and outbound messages.
   Notifications are not sent for "Just Log" actions.
8. Click **Apply**.

Content Scanning

Content Scanning is a feature that performs deep scanning of attachments in email messages and web requests, such as PDF and Microsoft document files, for patterns of text and phrases. This allows organizations to use filter rules and policy settings to scan attachments for specific content that could be considered offensive, private and confidential, or against existing compliance rules.

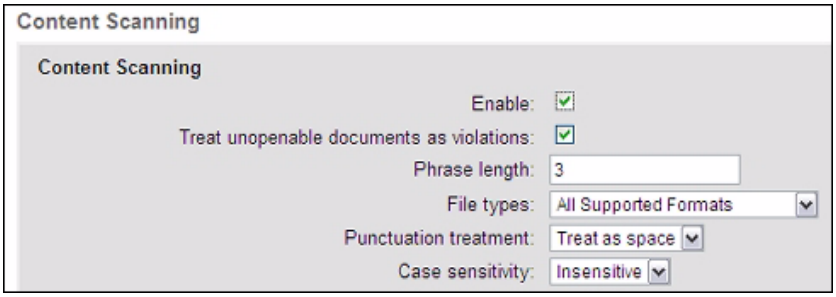
There are two content scanning methods for message attachments:

- A Pattern Filter is used to search for text and phrases in a document. If there is a match, an appropriate action is taken.
- The extracted message text is searched for words that are included in the Content Scanning dictionary files, which are defined in a policy. If there is a match, the configured action is taken.

Configure Content Scanning

To configure Content Scanning:

1. Select **Security > Content Control > Content Scanning**.



2. Select the **Enable** check box.
3. Select the **Treat unopenable documents as violations** check box to treat unopenable documents as though they were not compliant.
   Attachments that are protected by a password or encrypted cancontain text that is a compliance violation.
4. Specify the **Phrase Length** used for pattern-matching checks.
   This number of words will be passed to the scanning engine to check if it matches any phrases in your compliance file.

> *Long phrases will result in greater processing times. We recommend that phrases be four words or less. The phrase length of the compliance dictionary selected for Content Scanning should not be greater than the phrase length selected in this field. A phrase length of four must be used with the default Financial and Medical dictionaries and Credit Card pattern filters.*

5. Select the **File Types** to be scanned.
   - **All Supported Formats** — Scans all file formats supported by the content scanner.
   - **Common Document Formats** — Scans only common word processing, spreadsheet, database, presentation, text, and archive formats.
   - **Standard Document Formats** — Scans only common document formats (word processing, spreadsheet, database, presentation, text, and archive files), including less common formats, such as graphics and desktop publishing formats.

6. Select the type of **Punctuation Treatment**.
   - **Significant** — The punctuation is considered as part of the word or phrase it appears in.
   - **Treat as space** — The punctuation is treated as a space. For example, the phrase "This, is classified" is treated as "This is classified". This is the default setting.
   - **Ignore** — The punctuation is completely ignored.
7. Select how you want the scanning engine to treat **Case Sensitivity**.
   If **Sensitive** is chosen, capitalization of letters is taken into account. For example, the word "Classified" must appear in the phrase compliance file with the first letter capitalized.
8. Enable and customize **Notifications** for inbound and outbound messages.
   Notifications are not sent for "Just Log" actions.
9. Click **Apply**.

Use Pattern Filters for Content Scanning

One of the methods that can be used to search for compliance text in a file is to create a pattern filter.

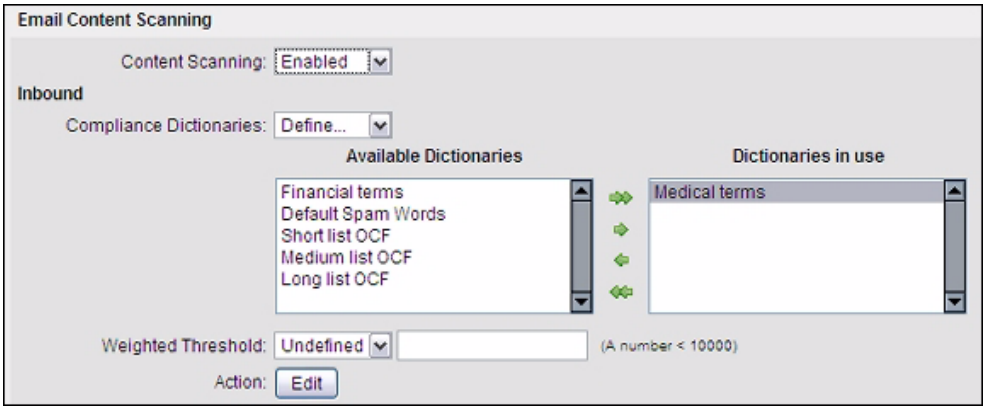
To create a pattern filter:

1. Select **Security** > **Content Control > Pattern Filters**.
2. Click **Add**.
3. In the **Apply To** field, select whether you want to check **Inbound**, **Outbound**, or **All Mail**.
4. In the **Message Part** field, select **Content Scanning**.
5. In the **Pattern** field, type a pattern to match against.
6. Select the **Action** to take on a message that contains the pattern text, such as **Reject**.
7. Click **Apply** to add the filter.

Use a Policy compliance dictionary for Content Scanning

Content scanning can also be enabled in policies when compliance dictionaries are uploaded and enabled. The compliance dictionaries contain a list of words and phrases that are checked against text in scanned attachment files and web uploads and downloads.

1. Select **Security > Policies > Policies**.
2. Select the policy you want to configure.
3. Select **Content Control**.
4. Go to the *Content Scanning* section.
5. Enable **Content Scanning**.



6. From the **Compliance Dictionaries** drop-down list, select **Define**.

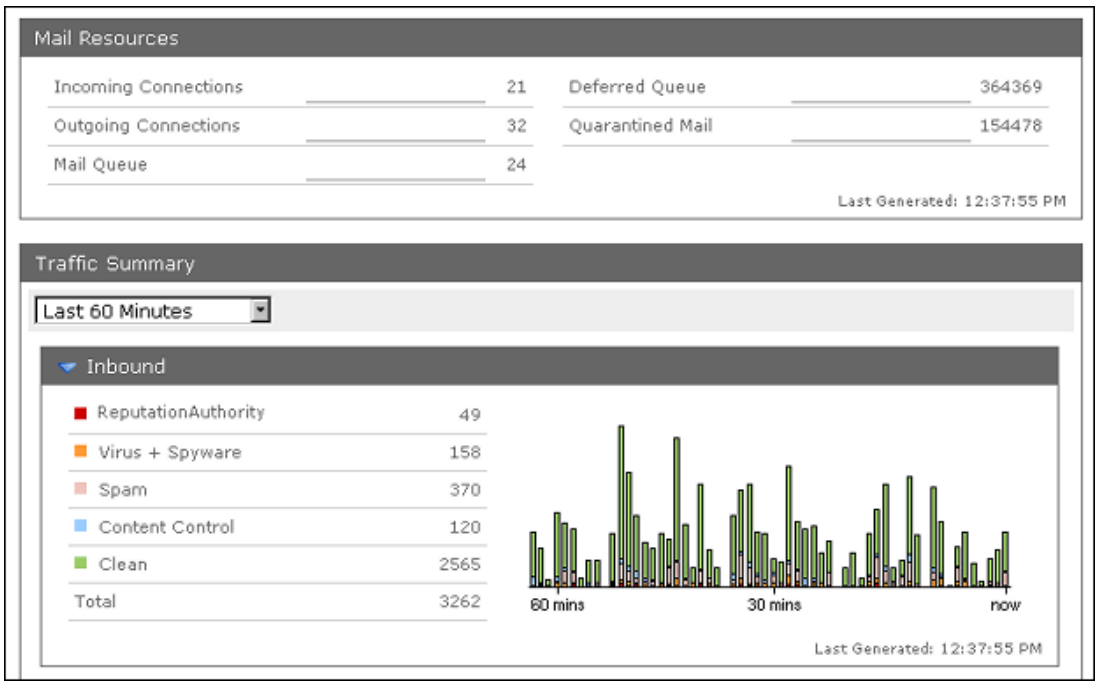
7. Select the dictionaries to use with Content Scanning.
8. In the **Action** field, click **Edit** and select the corresponding action to perform, such as **Reject**.
9. Click **Apply**.

11 Monitor the WatchGuard XCS

Dashboard

The WatchGuard XCS system *Dashboard* provides administrators with a brief statistical and graphical summary of current inbound and outbound email and web activity, as well as the XCS device itself.

To see the Dashboard, go to **Activity > Status > Dashboard**.



The Dashboard contains links to the following components:

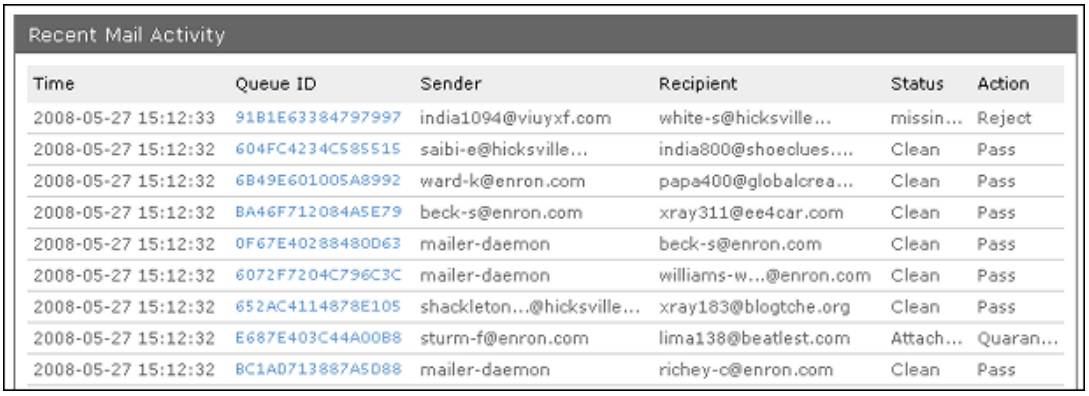
- **Mail Summary** — Shows information on mail resources, such as current incoming and outgoing connections, and the number of messages in the Mail, Deferred, and Quarantined queues. The Mail Summary screen also provides a traffic summary of inbound and outbound mail traffic separated by category (such as Virus, Spam, and Clean mail).

- **Web Summary** — Displays a web traffic summary separated by category (such as URL Categorization and Spyware). The Web Summary screen also provides information on the number of current active web connections, the web cache efficiency, the top five blocked web sites and IP Addresses/Users, and top five browsing users and visited domains.
- **Recent Mail Activity** — Displays the most recent mail messages that have been processed by the system, including the Message ID, Sender and Recipient information, the message Status, and the final Action taken on the message.
- **Recent Web Activity** — Displays the most recent blocked web messages that have been processed by the system, including the Request ID, Request To and From information, the message Status, and the final Action taken on the request.

Recent mail activity

The *Recent Mail Activity* screen displays information on the most recent mail messages that have passed through the system. The data updates every 60 seconds and also updates when the screen is refreshed.

- **Time** — The timestamp to show when the message was processed by the system.
- **Queue ID** — Each message that passes through the system is identified by a unique message identification number. Click the **Queue ID** of the message to see the details of the message processing.
- **Sender** — Shows the email address of the sender of the mail message.
- **Recipient** — Shows the email address of the recipient of the mail message.
- **Status** — Shows which feature acted upon the message if a security or content check was triggered. For example, "OCF" indicates that the message was acted on by the Objectionable Content Filtering feature.
- **Action** — Shows the final action that was performed on the message after it was processed, such as "Reject".


Recent Mail Activity

Time	Queue ID	Sender	Recipient	Status	Action
2008-05-27 15:12:33	91B1E63384797997	india1094@viuyxf.com	white-s@hicksville...	missin...	Reject
2008-05-27 15:12:32	604FC4234C585515	saibi-e@hicksville...	india800@shoeclues....	Clean	Pass
2008-05-27 15:12:32	6B49E601005A8992	ward-k@enron.com	papa400@globalcrea...	Clean	Pass
2008-05-27 15:12:32	BA46F712084A5E79	beck-s@enron.com	xray311@ee4car.com	Clean	Pass
2008-05-27 15:12:32	0F67E40288480D63	mailer-daemon	beck-s@enron.com	Clean	Pass
2008-05-27 15:12:32	6072F7204C796C3C	mailer-daemon	williams-w...@enron.com	Clean	Pass
2008-05-27 15:12:32	652AC4114878E105	shackleton...@hicksville...	xray183@blogtche.org	Clean	Pass
2008-05-27 15:12:32	E687E403C44A00B8	sturm-f@enron.com	lima138@beatlest.com	Attach...	Quaran...
2008-05-27 15:12:32	BC1AD713887A5D88	mailer-daemon	richey-c@enron.com	Clean	Pass

Reports

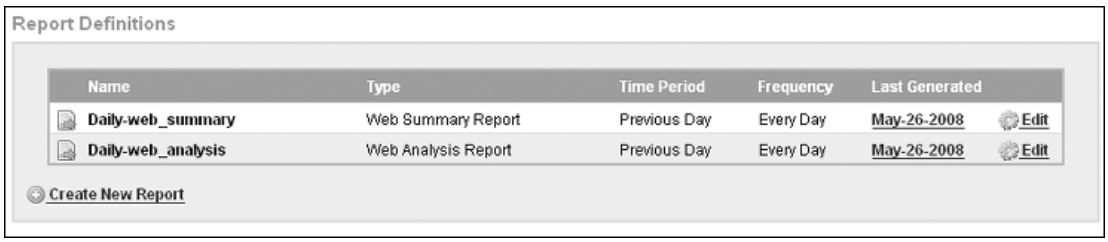
The WatchGuard XCS reporting functionality provides a comprehensive range of informative reports. You can generate reports on demand and at scheduled times. Reports are created from information written to the message log files and stored in the database. You can store up to one month of reporting data and see it online, depending on message loads for a particular environment.

The XCS stores reports on the system for online viewing, and the reports can also be emailed automatically to the XCS administrator. You can generate reports in PDF (Adobe Portable Document Format), CSV, and HTML format.

Schedule reports

To schedule and generate reports:

1. Select **Activity > Reports > Schedule**.

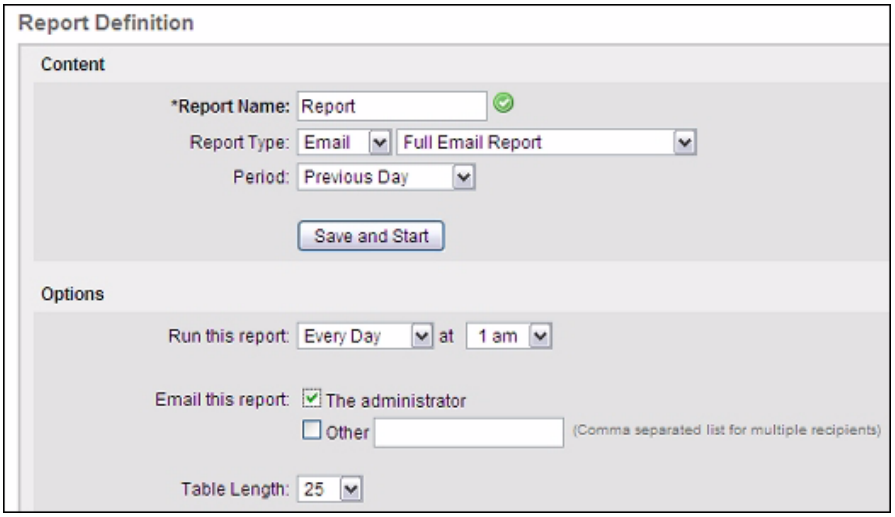


   The *Report Definitions* screen displays any scheduled and defined reports, including the report name, report type, the report time period, the frequency, and the last time the report was generated.
2. Click the **Edit** link to edit an existing report, or click the **Create New Report** link to create a new report definition.
3. Click the **Last Generated** date link to see the last generated report from this report definition.

Create a new report

To create a new report:

1. Click the **Create New Report** link.



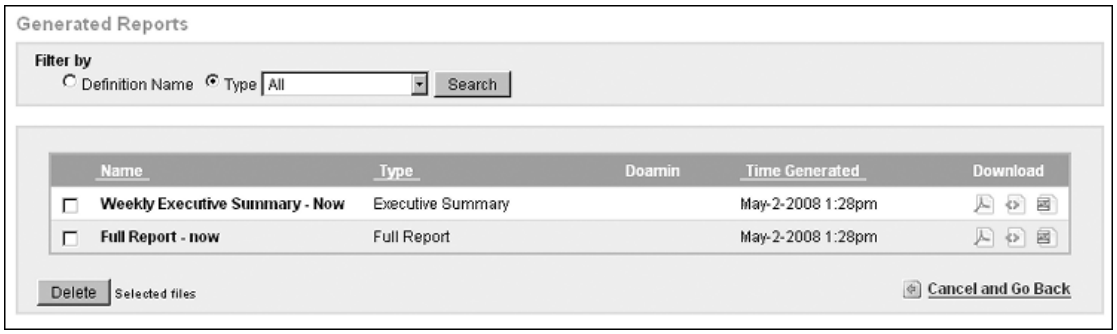
2. Enter a descriptive **Report Name** for this report.
   Use only alphanumerical letters, numbers, and spaces in the name. Do not use any special characters.
3. Select the specific **Report Type** to run for this report.
4. Select a category of reports, such as **Email**, **Web**, and **System**, and then choose a report sub-type for that category.
5. Select the time **Period** for the report coverage:
   - **Previous Day** (includes up to midnight of the previous day)
   - **Last 7 Days**
   - **Sunday–Saturday** (includes 7 days from a Sunday to the next Saturday)
   - **Monday–Friday** (includes 5 days from Monday to Friday)
   - **Previous Month** (this is the previous calender month).

   *To report on the previous month in a report definition, the Reporting Summary Days option in **Configuration > Miscellaneous > Reports** must be set to 60 days or more to have enough data to cover the previous month time period.*
6. In the **Run this report** field, select the day and time to run the scheduled report.
7. In the **Email this report** section, select who to send a copy of the report to when it is generated.
   Select **The administrator** to send it to the administrator of this system, and/or select **Other** and enter a comma-separated list of addresses to send the report to, such as:
   `admin@example.com, admin2@example.com, admin3@example.com`
8. Select the **Table Length** for each report field.
   For example, in the Top Viruses list, the top 50 viruses are displayed if this field is set to 50. The default is 25. This default value is configurable through **Configuration > Miscellaneous > Reports**.
9. Click **Save and Start** to save the report and generate it immediately.
   Select **Save** or **Save As** (to save under a different name) to save the report and run it at the scheduled time and day.
   Click **Delete** to remove this report definition. Any reports associated with this report definition are not deleted and can still be viewed.

View reports

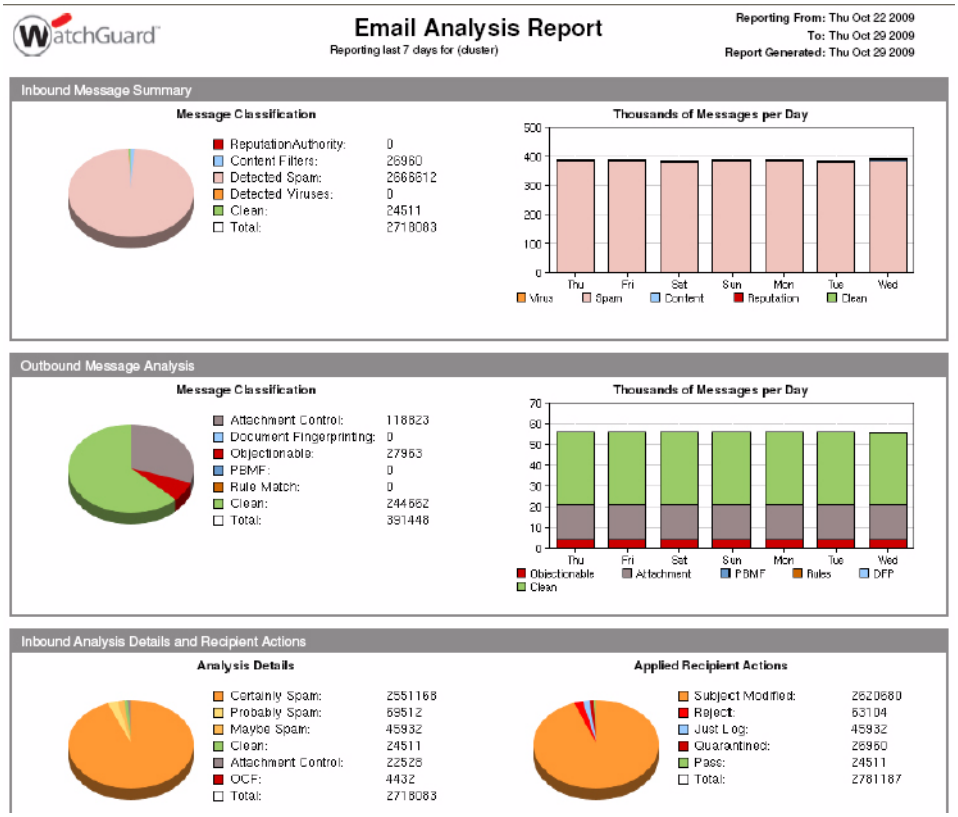
To view your generated reports:

1. Select **Activity > Reports > View**.



Reports are generated in PDF (Adobe Portable Document Format), CSV, and HTML format.

2. Click the appropriate icon to see the contents of the report in the specified format.
The report either appears in a new browser window (for an HTML report) or the PDF and CSV versions of the report can be saved on the local computer.



Email Analysis Report

Reporting last 7 days for (cluster)

Reporting From: Thu Oct 22 2009
To: Thu Oct 29 2009
Report Generated: Thu Oct 29 2009

Inbound Message Summary

Message Classification

ReputationAuthority:	0
Content Filters:	26960
Detected Spam:	2668612
Detected Viruses:	0
Clean:	24511
Total:	2718083

Thousands of Messages per Day

Outbound Message Analysis

Message Classification

Attachment Control:	116823
Document Fingerprinting:	0
Objectionable:	27963
PBMF:	0
Rule Match:	0
Clean:	244662
Total:	391448

Thousands of Messages per Day

Inbound Analysis Details and Recipient Actions

Analysis Details

Certainly Spam:	2551168
Probably Spam:	69512
Maybe Spam:	45932
Clean:	24511
Attachment Control:	22528
OCF:	4432
Total:	2718083

Applied Recipient Actions

Subject Modified:	2620680
Reject:	63104
Just Log:	45932
Quarantined:	26960
Pass:	24511
Total:	2781187

Message History

Each message that passes through the WatchGuard XCS generates a database entry that records information about how it was processed, filtered, and delivered. To see how the message was processed, you can examine the message history database to see the disposition of the message.

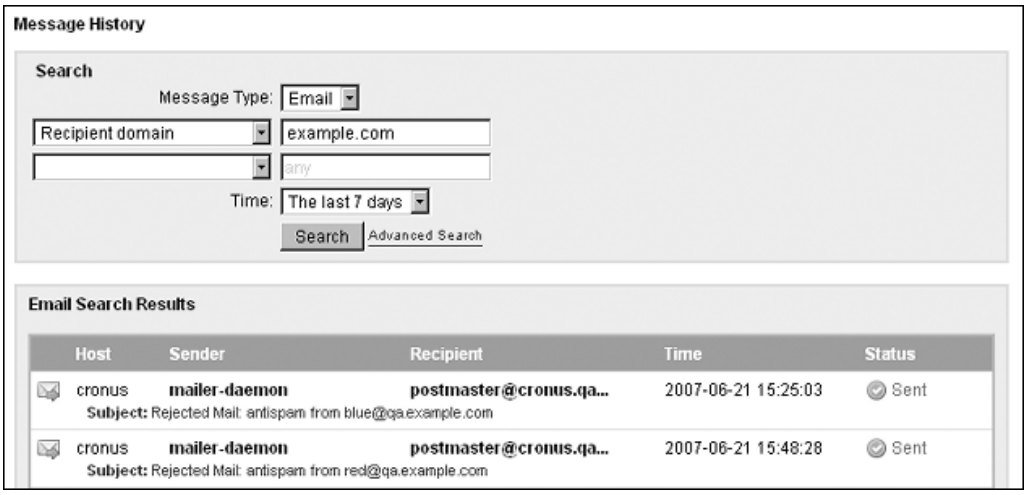
To see the message history:

1. Select **Activity > History > Message History**.
2. Examine the **Status** column for full information on how a message was processed and its final disposition.
3. Use the search fields to filter the message history results.

   All simple search fields default to exact matches, except for "Subject" that accepts partial matches, and "Domain part" that matches the ending of a domain part. For more detailed and flexible searches, use the **Advanced Search** option.

   You can also perform the following actions:

   - Click the **Download these results** link to save the search results as a local file.
   - Click on a **Message ID** to view the details of the message.
   - Click the **Show Log** button to see the corresponding log entry for this message.

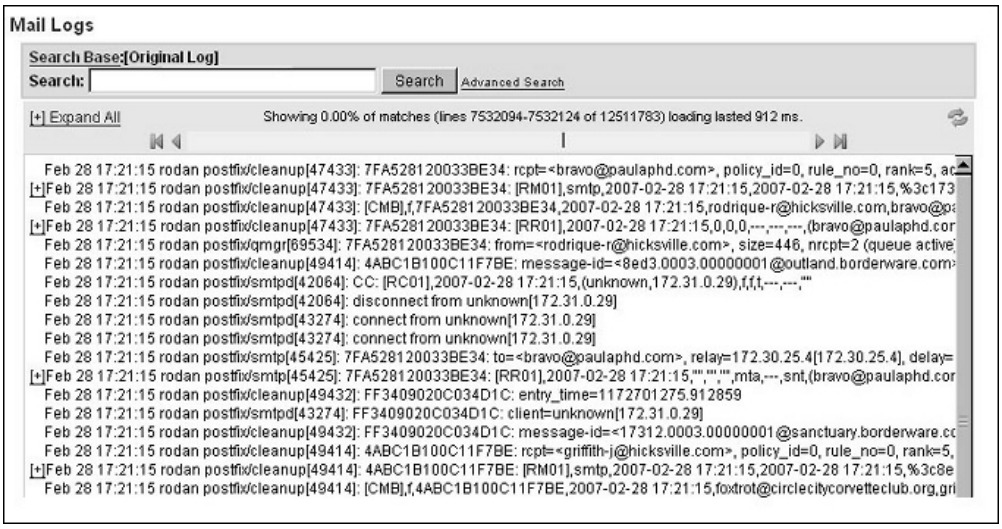


Mail Logs

The Mail Logs are the most important and informative log messages to monitor because they contain a record of all mail messages processed by the system.

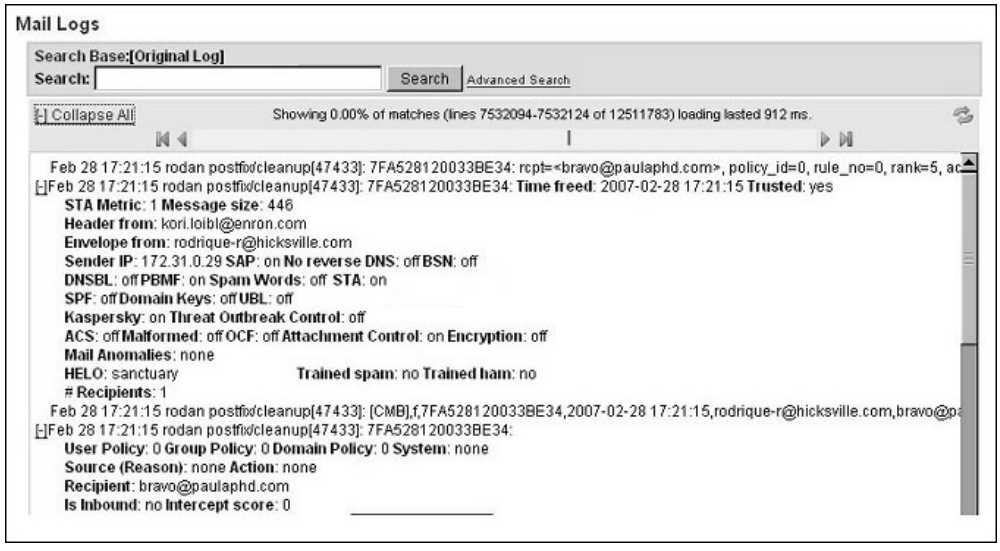
To get access to the WatchGuard XCS Mail Logs:

1. Select **Activity > Logs > Mail**.
   The screen displays the end of the log file.
2. Use the slider control to page through the log file, or use the right and left arrow icons. You can also jump to the start or end of the log file with the arrow icons as required.


Mail Logs
Search Base:[Original Log]
Search:
Search
Advanced Search
[+] Expand All
Showing 0.00% of matches (lines 7532094-7532124 of 12511783) loading lasted 912 ms.
Feb 28 17:21:15 rodan postfix/cleanup[47433]: 7FA528120033BE34: rcpt=<bravo@paulaphd.com>, policy_id=0, rule_no=0, rank=5,
[+]Feb 28 17:21:15 rodan postfix/cleanup[47433]: 7FA528120033BE34: [RM01],smtp,2007-02-28 17:21:15,2007-02-28 17:21:15,%3c173
Feb 28 17:21:15 rodan postfix/cleanup[47433]: [CMB],f,7FA528120033BE34,2007-02-28 17:21:15,rodrique-r@hicksville.com,bravo@p
[+]Feb 28 17:21:15 rodan postfix/cleanup[47433]: 7FA528120033BE34: [RR01],2007-02-28 17:21:15,0,0,0,---,---,---,(bravo@paulaphd.cor
Feb 28 17:21:15 rodan postfix/qmgr[69534]: 7FA528120033BE34: from=<rodrique-r@hicksville.com>, size=446, nrcpt=2 (queue active)
Feb 28 17:21:15 rodan postfix/cleanup[49414]: 4ABC1B100C11F7BE: message-id=<8ed3.0003.00000001@outland.borderware.com>
Feb 28 17:21:15 rodan postfix/smtpd[42064]: CC: [RC01],2007-02-28 17:21:15,(unknown,172.31.0.29),f,f,t,---,---,""
Feb 28 17:21:15 rodan postfix/smtpd[42064]: disconnect from unknown[172.31.0.29]
Feb 28 17:21:15 rodan postfix/smtpd[43274]: connect from unknown[172.31.0.29]
Feb 28 17:21:15 rodan postfix/smtpd[43274]: connect from unknown[172.31.0.29]
Feb 28 17:21:15 rodan postfix/smtp[45425]: 7FA528120033BE34: to=<bravo@paulaphd.com>, relay=172.30.25.4[172.30.25.4], delay=
[+]Feb 28 17:21:15 rodan postfix/smtp[45425]: 7FA528120033BE34: [RR01],2007-02-28 17:21:15,"","","",mta,---,snt,(bravo@paulaphd.cor
Feb 28 17:21:15 rodan postfix/cleanup[49432]: FF3409020C034D1C: entry_time=1172701275.912859
Feb 28 17:21:15 rodan postfix/smtpd[43274]: FF3409020C034D1C: client=unknown[172.31.0.29]
Feb 28 17:21:15 rodan postfix/cleanup[49432]: FF3409020C034D1C: message-id=<17312.0003.00000001@sanctuary.borderware.co
Feb 28 17:21:15 rodan postfix/cleanup[49414]: 4ABC1B100C11F7BE: rcpt=<griffith-j@hicksville.com>, policy_id=0, rule_no=0, rank=5,
[+]Feb 28 17:21:15 rodan postfix/cleanup[49414]: 4ABC1B100C11F7BE: [RM01],smtp,2007-02-28 17:21:15,2007-02-28 17:21:15,%3c8e
Feb 28 17:21:15 rodan postfix/cleanup[49414]: [CMB],f,4ABC1B100C11F7BE,2007-02-28 17:21:15,foxtrot@circlecitycorvetteclub.org,gri

The start of a single message log entry begins with a connect message, and ends with the disconnect message. Check the message ID (such as 7FA528120033BE34 in the previous example) for each log entry to make sure they are for the same message.

3. Click **Expand All** to show a summary of the processing for a message.


Mail Logs
Search Base:[Original Log]
Search:
Search
Advanced Search
[-] Collapse All
Showing 0.00% of matches (lines 7532094-7532124 of 12511783) loading lasted 912 ms.
Feb 28 17:21:15 rodan postfix/cleanup[47433]: 7FA528120033BE34: rcpt=<bravo@paulaphd.com>, policy_id=0, rule_no=0, rank=5,
[-]Feb 28 17:21:15 rodan postfix/cleanup[47433]: 7FA528120033BE34: Time freed: 2007-02-28 17:21:15 Trusted: yes
STA Metric: 1 Message size: 446
Header from: kori.loibl@enron.com
Envelope from: rodrique-r@hicksville.com
Sender IP: 172.31.0.29 SAP: on No reverse DNS: off BSN: off
DNSBL: off PBMF: on Spam Words: off STA: on
SPF: off Domain Keys: off UBL: off
Kaspersky: on Threat Outbreak Control: off
ACS: off Malformed: off OCF: off Attachment Control: on Encryption: off
Mail Anomalies: none
HELO: sanctuary Trained spam: no Trained ham: no
Recipients: 1
Feb 28 17:21:15 rodan postfix/cleanup[47433]: [CMB],f,7FA528120033BE34,2007-02-28 17:21:15,rodrique-r@hicksville.com,bravo@p
[-]Feb 28 17:21:15 rodan postfix/cleanup[47433]: 7FA528120033BE34:
User Policy: 0 Group Policy: 0 Domain Policy: 0 System: none
Source (Reason): none Action: none
Recipient: bravo@paulaphd.com
Is Inbound: no Intercept score: 0

Search the Mail Logs

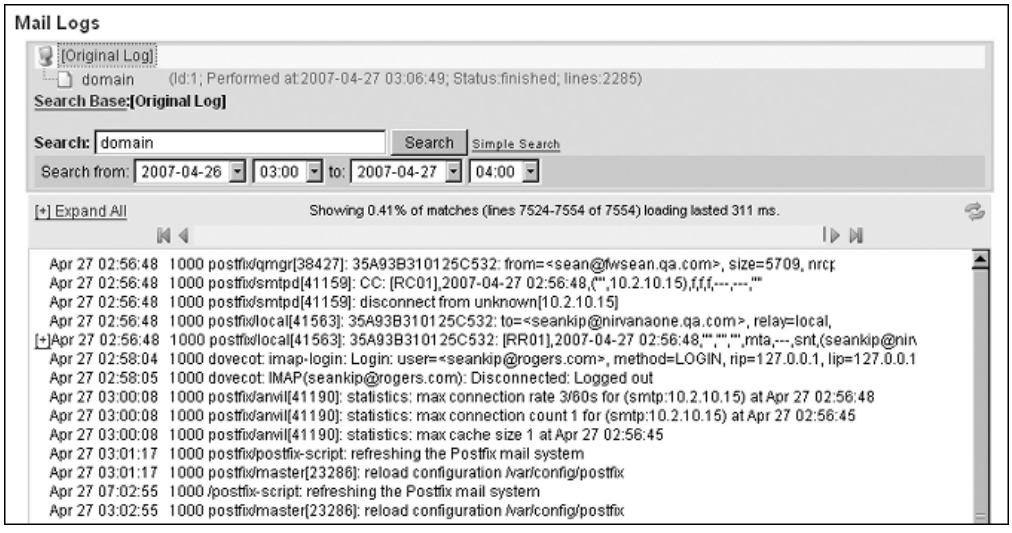
To search the Mail Logs:

1. Enter a text string in the **Search** field.
2. Click **Search** to filter the results.
   Multiple searches can be added on to the original search to filter the results further.
3. Click **Remove** to remove the previous search base, or click **Search Base (Original Log)** to start a new search again.

Mail Logs
[Original Log]
error (Id:1; Performed at:2007-03-13 11:12:54; Status:finished; lines:129)
domain (Id:2; Performed at:2007-03-13 11:14:11; Status:finished; lines:122)
Search Base:[Original Log] > error > domain
Search: domain
Search
Advanced Search
[+] Expand All
Showing 25.41% of matches (lines 92-122 of 122) loading lasted 260 ms.

By default the search only applies to the last 24 hours of log entries.

4. Use the **Advanced Search** to modify the specific time period for the search.


Mail Logs
[Original Log]
domain (Id:1; Performed at:2007-04-27 03:06:49; Status:finished; lines:2285)
Search Base:[Original Log]
Search: domain
Search
Simple Search
Search from: 2007-04-26 03:00 to: 2007-04-27 04:00
[+] Expand All
Showing 0.41% of matches (lines 7524-7554 of 7554) loading lasted 311 ms.

12 System Administration

Backup and Restore

The WatchGuard XCS can back up all data, including the report database, quarantined items, mail queues, user mail directories, uploaded user lists, SSL certificates, feature keys, and system configuration data.

The system supports three backup methods:

- FTP server (recommended for large, full backups)
- SCP (Secure Copy) server
- Local disk (for small size or partial configuration backups with a browser download to a workstation)

> ! *We strongly recommend that the FTP backup method be used for large backup requirements. Local Disk backups should only be used for small, partial configuration backups. The system cannot restore a local backup file more than 2GB in size.*

Restore from backup

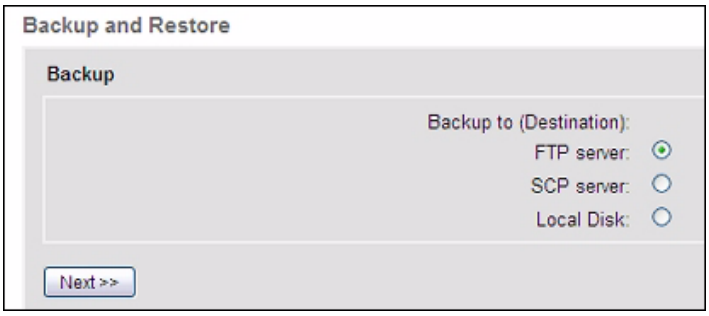
The restore feature can restore any backup items individually. The system should be backed up before performing any type of software upgrade or update. The restore operation restores the configuration and report data in two separate stages.

- **Configuration restore** — The system configuration is restored first. This process takes only a short amount of time and the user can quickly return to the administrative user interface to start to process messages again. A critical alarm "Critical Restore: Complete PASSED" is generated to alert the administrator when this first stage of the restore is complete.
- **Reporting data restore** — The report data (if required) is then restored as a background process. This can be performed while the system processes messages. When you restore report data on a running system, it can take 24 to 72 hours before the restore is fully completed, depending on the amount of data that you restore. The following serious alarms are generated at different points in the reporting restore process:
  - "Serious: RESTORE: Reporting: Recovery Started": This shows that the online reporting restore process has started and data is being copied into a temporary database.
  - "Serious: RESTORE: Reporting: Migration Started": This shows the data has been fully copied into the temporary database and is being migrated to the online database.
  - "Serious: RESTORE: Reporting: Recovery Complete": This shows that the online reporting restore process has completed.

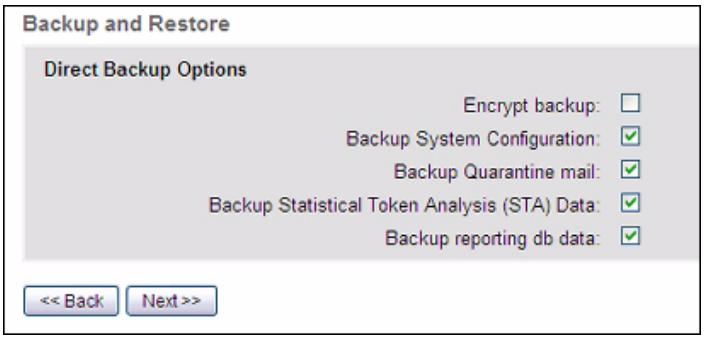
Start a backup

To start a local disk backup:

1. Select **Administration > Backup/Restore > Backup & Restore**.

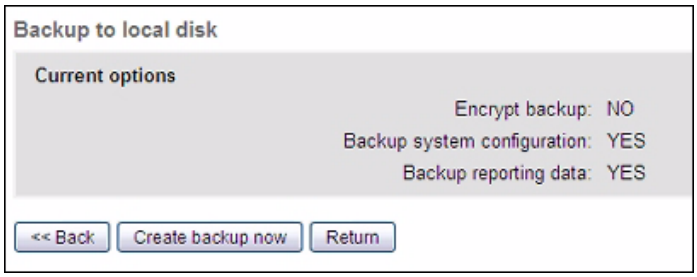


Select the **Local Disk** backup destination and click **Next>>**.



- **Encrypt Backup** — Select this check box to store the backup file in encrypted form.
- **Backup System Configuration** — Select this check box to back up all system configuration data, including mailboxes, licenses, and keys. This option must be enabled if you want to restore system functionality.
- **Backup Quarantine Mail** — Select this check box to back up all quarantined mail. This can greatly increase the size of the backup file.
- **Backup Token Analysis Data** — Select this check box to back up the Token Analysis database.
- **Backup Reporting Data** — Select this check box to back up the entire report database. This can greatly increase the size of the backup file. It is recommended that FTP for SCP methods be used for very large backup files.

2. When you have set your options, click **Next >>** to continue.

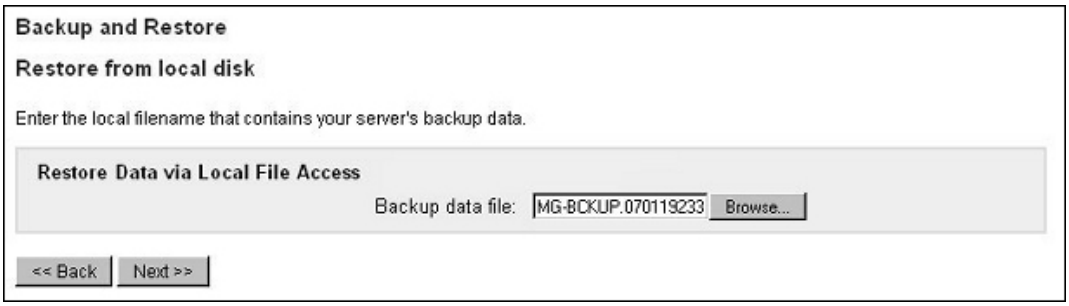


3. Verify that your options are correct, and then click **Create backup now** to start the backup.
The system prompts you for a location to download the file (backup.gz). The backup file is saved in a gzip compressed archive.

Restore a backup

To restore from a local disk backup file:

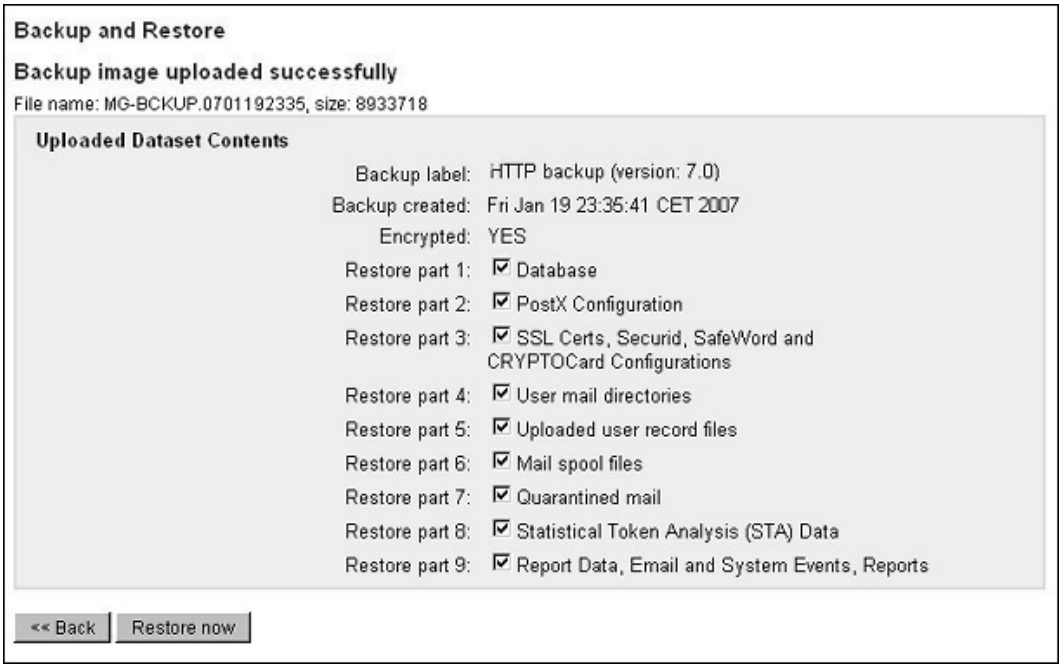
1. Select **Administration > Backup/Restore > Backup & Restore**.
2. Select the **Local Disk** restore method and click **Next >>**.
3. Type the local file name that contains your server's backup data, or click **Browse** to select the file from the local drive directory.
4. Click **Next >>** to upload and restore the backup file.



You can see the current status of the restore process in the **Status** section of the **Administration > Backup/Restore > Backup and Restore** page.

5. When the backup file has been successfully retrieved, you can choose which aspects of the system you want to restore.

   After you select the items you want to restore, click **Restore Now**.

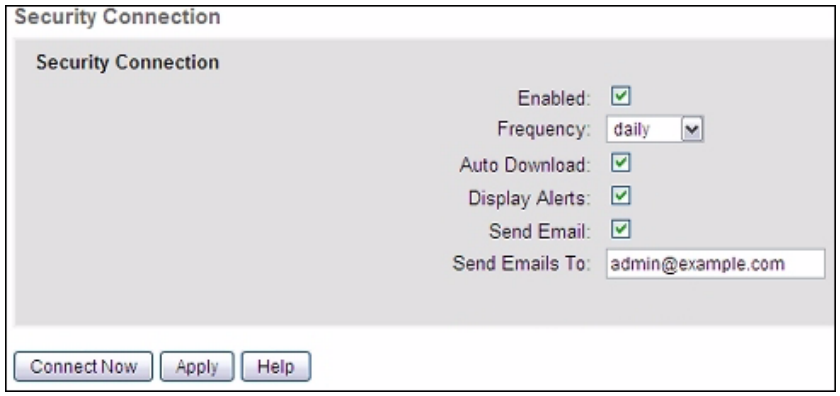

Backup and Restore
Backup image uploaded successfully
File name: MG-BCKUP.0701192335, size: 8933718
Uploaded Dataset Contents
Backup label: HTTP backup (version: 7.0)
Backup created: Fri Jan 19 23:35:41 CET 2007
Encrypted: YES
Restore part 1: Database
Restore part 2: PostX Configuration
Restore part 3: SSL Certs, Securid, SafeWord and CRYPTOCard Configurations
Restore part 4: User mail directories
Restore part 5: Uploaded user record files
Restore part 6: Mail spool files
Restore part 7: Quarantined mail
Restore part 8: Statistical Token Analysis (STA) Data
Restore part 9: Report Data, Email and System Events, Reports
<< Back
Restore now

Security Connection

The Security Connection is a service that polls WatchGuard's support servers for new updates, security alerts, and Anti-Spam database updates. When new information and updates are received, a notification can be sent to the administrator.

To connect to Security Connection:

1. Select **Administration > Software Updates > Security Connection**.



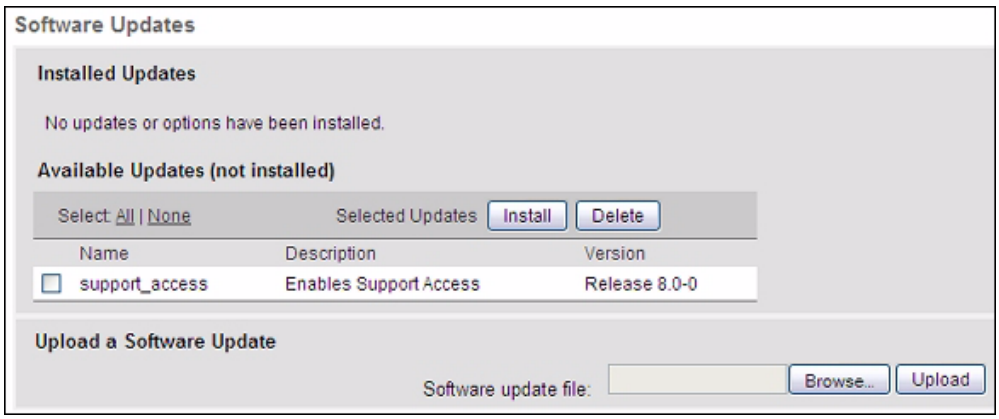
2. Select the **Enabled** option.
3. Specify the **Frequency** for how often to run the Security Connection service.
   Choices are daily, weekly, and monthly.
4. Enable the **Auto Download** option to allow software updates to be downloaded automatically.
   These updates are NOT automatically installed. They must be installed manually through Software Updates.
5. Enable the **Display Alerts** option to display any Security Connection alert messages on the system console.
6. Enable the **Send Email** option to send an email to the address specified in the **Send Emails To** field.
7. In the **Send Emails To** text box, enter an email address to receive notifications.
8. Click **Apply**.
9. Click **Connect Now** to run Security Connection immediately and check for new software updates.

Software Updates

To make sure your system software is up to date with the latest patches and upgrades, you must install any updates released for your version of software. The Security Connection, if enabled, downloads any required software updates automatically.

To upload and install software updates:

1. Select **Administration > Software Updates > Updates**.
   The Software Updates screen shows updates that are *Available Updates* (loaded onto the system, but not applied) and *Installed Updates* (applied and active.) You can install an available update or uninstall a previously installed update. Software updates downloaded from Security Connection appear in the *Available Updates* section.



2. If you downloaded your software update manually:
   - Click **Browse**.
   - Navigate to the downloaded software update on your local system.
   - Click **Upload**. The software update now appears in the *Available Updates* section.
3. Select the software update in the *Available Updates* section.
4. Click **Install**.
   After you apply any updates, you must restart the system.

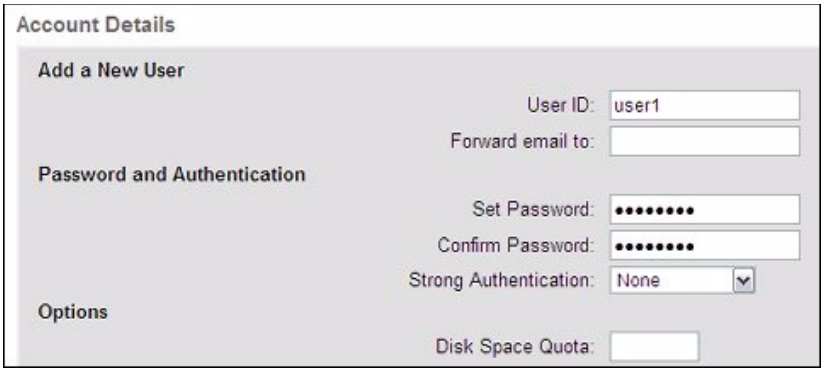
Local Accounts and Tiered Administration

To add new local users:

1. Select **Administration > Accounts > Local Accounts**.

> *Local users are not available on cluster systems, except for admin users.*

2. Click **Add**.



3. In the **User ID** field, type an RFC821 compliant mail box name for the user.
4. In the **Forward email to** field, type an optional address to forward all mail to.
5. type and confirm the user's **Password**.
   The user should change this password the first time they log in. If Strong Passwords are enabled, the password must be at least 6 characters and contain alphabetic and non-alphabetic characters.
6. Select a **Strong Authentication** method, if required.
7. Enter an optional user **Disk Space Quota** in megabytes (MB). Enter a value of "0" for no quota.
8. Select the **Accessible IMAP/WebMail Servers** that this user can access.
9. Click **Create**.

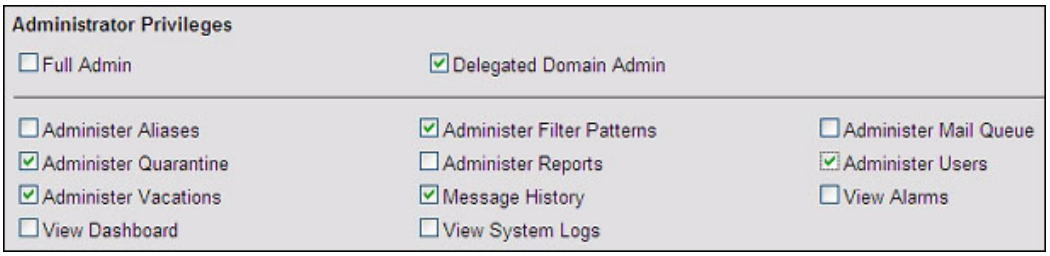
Tiered administration

Tiered Administration allows an administrator to assign additional administrative access permissions on a per-user basis. For example, the administrator can designate another user as an alternate administrator when they select the Full Admin option in the user profile. To distribute administrative functions, the administrator can configure more selective permissions to authorize a user only for certain tasks, such as user administration, report administration the ability to configure Anti-Spam filter patterns, or the ability to see the Message History database.

To enable administrator permissions:

1. Select **Administration > Accounts > Local Accounts**.
2. Select a user account.

3. Select the corresponding check box to enable each administrative option as required for that user.



Full Admin
The user has administrative privileges equivalent to the admin user.

Administer Aliases
The user can add, edit, remove, upload, and download aliases (not including LDAP aliases.)

Administer Filter Patterns
The user can add, edit, remove, upload, and download Pattern Filters and Specific Access Patterns.

Administer Mail Queue
The user can administer mail queues.

Administer Quarantine
The user can view, delete, and send quarantined files.

Administer Reports
The user can view, configure and generate reports, and view system activity.

Administer Users
The user can add, edit, and relocate user mailboxes (except the Full Admin users), including the upload and download of user lists. The user can also configure user vacation notifications.

Administer Vacations
The user can edit local user vacation notification settings and other global vacation parameters.

Message History
The user can view the Message History database and perform quick searches of the recent Mail and Web activity on the Dashboard.

View Dashboard
The user can view the Dashboard page. Tiered admins can only perform a quick search of the recent Mail and Web activity if Message History is also enabled.

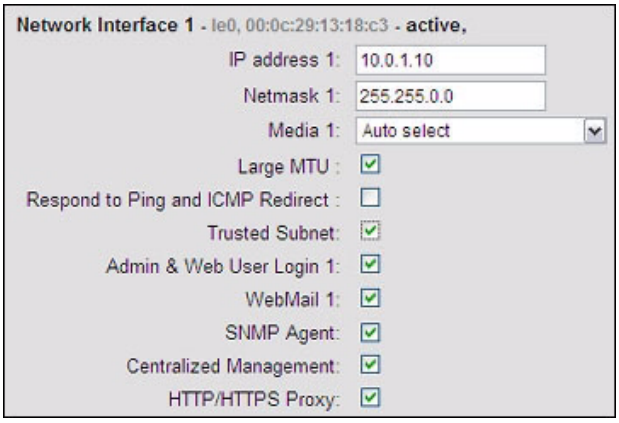
View Alarms
The user can view the Alarms in the Alarms Indicator and the Local Alarms screen, but cannot acknowledge them.

View System Logs
The user can view all system log files.

Tiered Admin and WebMail access

Tiered Admin and WebMail access must be enabled on a network interface to allow Tiered Admin users to log in and administer the system.

1. Select **Configuration > Network > Interfaces**.
2. Select the **Admin & Web User Login** and **WebMail** check boxes on the required network interface.

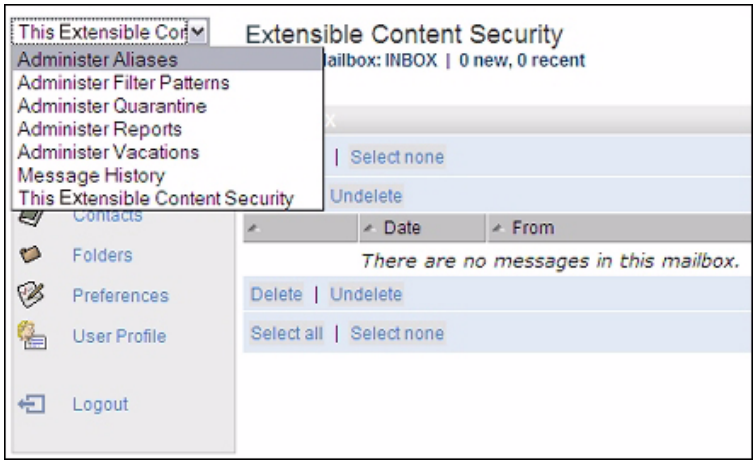


3. Click **Apply**.
   The system must be rebooted.

Log in with Tiered Admin privileges

When tiered administrative privileges have been assigned to a user, they can connect to the WebMail client interface.

1. Log in to the WatchGuard XCS.
2. Select the feature to administer through the top-left drop-down list.



13 Clustering and Queue Replication

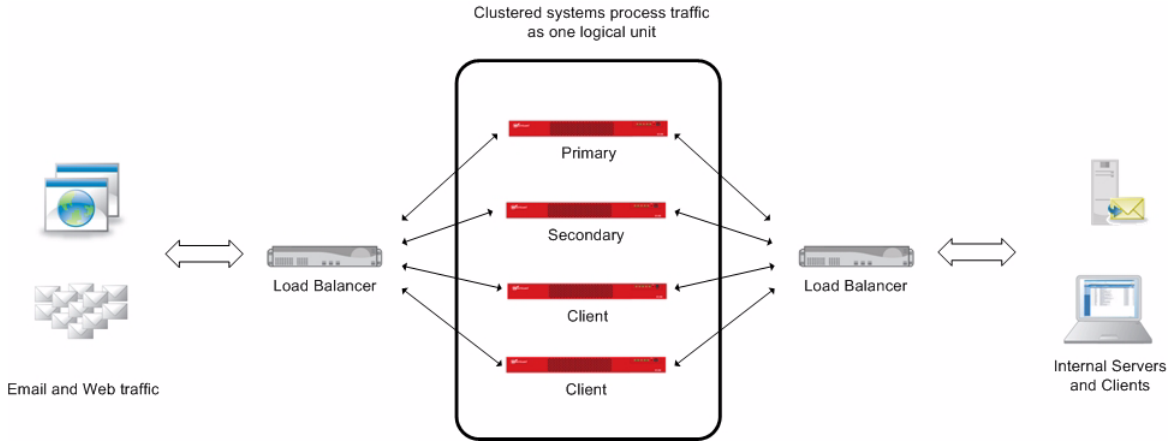
Clustering Overview

Clustering provides a highly scalable, redundant messaging security infrastructure that enables two or more WatchGuard XCS systems to act as a single logical unit to process messages and offers redundancy and high availability benefits.

There is no theoretical limit to the size of the cluster, and systems can be easily added to the cluster to increase processing and high-availability capabilities. With clustering, the flow of traffic is not interrupted because of individual system failures.

A cluster can be managed from any single system in the cluster without the need for a separate management console, and all systems in the cluster can process messages. Any configuration changes, such as Anti-Spam and Policies, are propagated to all systems in the cluster.

The WatchGuard XCS clustering architecture is illustrated in the following diagram.



The WatchGuard XCS can operate in one of four different modes in a cluster:

- **Primary** — This system is the primary master system for the cluster. All configuration is performed from this system. Other systems in the cluster pull configuration changes from the Primary system automatically when these changes are applied.

- **Secondary** — A system running in Secondary mode operates the same way as a Client cluster member except that it retains a copy of the master database replicated from the Primary system. In the event the Primary cluster member fails, the Secondary system can be promoted to Primary status.
- **Client** — A system running in Client mode pulls its configuration from an existing Primary system. After initial setup, no configuration is required on the Client system. A Client system can be promoted to a Secondary system. Unlike a Primary or Secondary system, a client does not contain a copy of the full configuration database.
- **Standalone** — The system initially installs in Standalone mode. In this mode, the system does not participate as part of the cluster and does not pull configuration updates, but is still able to process mail. This mode is primarily used to remove a cluster member for offline maintenance or software updates.

Load balancing

Although the cluster is treated as one logical system for processing messages, network traffic is processed independently by each cluster system and requires the use of a load balancing system to distribute mail flow between the systems in the cluster.

Email load balancing through DNS

A DNS round-robin technique can be used to distribute incoming SMTP mail connections through DNS to the systems in the cluster, as shown in the following example DNS MX records:

```
example.com IN MX 10 mail1.example.com
example.com IN MX 10 mail2.example.com
```

To give priority to specific servers, you can configure different priority values. For example:

```
example.com IN MX 5 mail1.example.com
example.com IN MX 10 mail2.example.com
```

Load balancing for specific types of network traffic (such as HTTP) cannot be performed through DNS round-robin techniques.

Traffic load balancing with a load balancing device

A hardware load balancing device can also be used to send messages to different systems in a cluster. If one of the systems fails, the load balancer will distribute the load between the remaining systems. The load balancer can be configured to distribute the mail stream connections intelligently across all systems in the cluster with techniques such as distribution by system load and availability.

External load balancing devices are mandatory if an organization must route specific traffic (such as SMTP and HTTP) through specific hosts in the cluster. For example, SMTP mail can be processed by two cluster systems, while HTTP is handled by two different systems. The load balancer can be configured to route protocol-specific traffic as required.

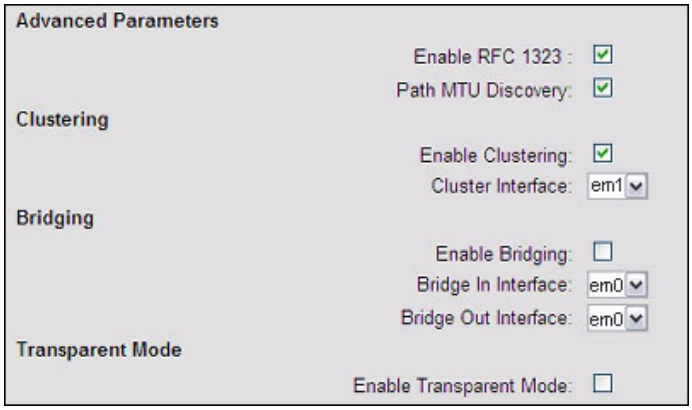
Configure Clustering

The following instructions describe how to configure the network settings for two systems in a cluster.

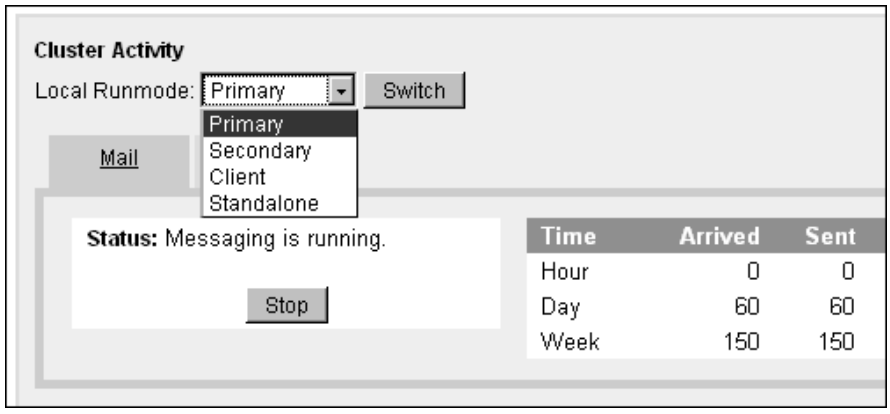
1. Connect an unused network interface from each system in the cluster to a common network switch, or connect each interface with a crossover network cable. This forms the cluster network, which is a control network in which clustering information is passed back and forth between the systems that form the cluster.

   For security reasons, this network should be isolated and not be connected to the main network. For a cluster of two systems, a crossover network cable can be connected between the selected interfaces to provide a secure connection without the need for a switch.
2. On each system, select **Configuration > Network > Interfaces**.
3. In the **Clustering** section of the Network Settings screen, select the **Enable Clustering** check box.
4. Select the network interface that is connected to the cluster network.

   This interface should not be configured with an IP address. The interface is automatically configured for exclusive use on the cluster network.



5. Make sure that an NTP time server is configured on each system (preferably more than one NTP server for redundancy).
   Clustering cannot be enabled until an NTP server is configured. The time server is used to make sure that all cluster systems are synchronized from a common time source.
6. Click **Apply**.
   The system must be rebooted after making changes to the networking configuration.
7. Select **Activity > Status > Cluster Activity**.



8. From the **Local Runmode** drop-down list, select **Primary**.

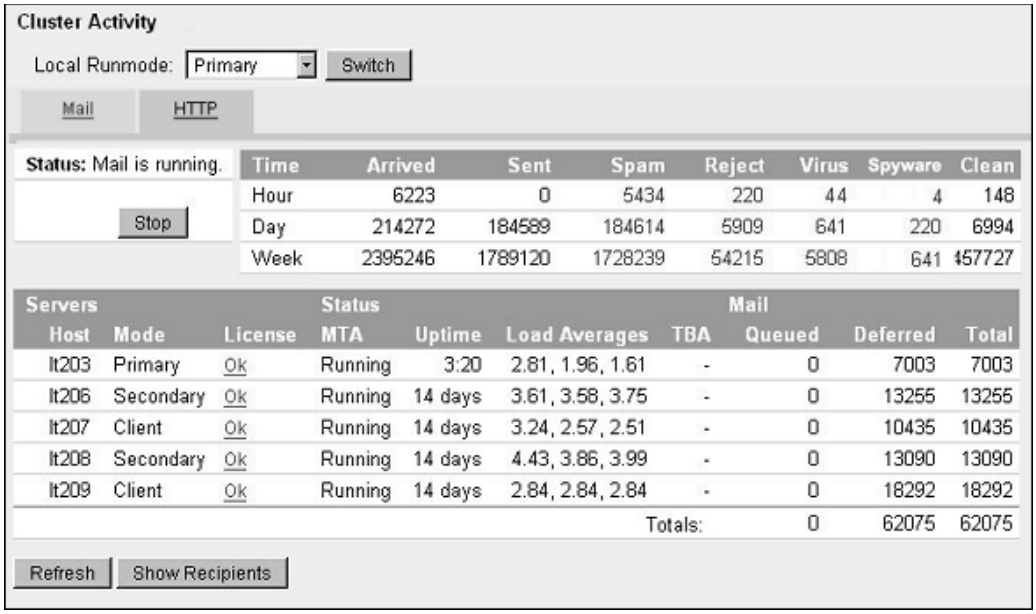
9. Click **Switch** to switch to the selected **Primary** mode.

   For your other cluster systems, you must configure at least one system as the Secondary system, while any other systems can be configured as a Secondary or Client. When systems are added to a cluster, the configuration of the Primary system is replicated automatically to the new cluster member.

10. When you have configured all of your clustered systems, the Cluster Activity page shows the mode and status of the other members of the cluster.

Cluster activity

When a system operates as part of a cluster, the Cluster Activity page displays processing statistics for the entire cluster. Select **Activity > Status > Local Activity** to see the statistics for this specific system only.

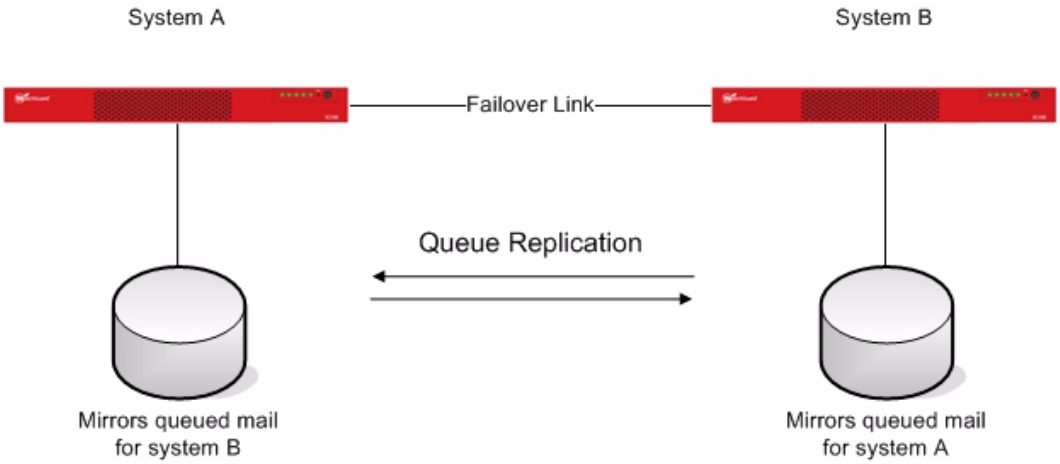

Cluster Activity
Local Runmode: Primary
Switch
Mail
HTTP
Status: Mail is running.
Stop
Time Arrived Sent Spam Reject Virus Spyware Clean
Hour 6223 0 5434 220 44 4 148
Day 214272 184589 184614 5909 641 220 6994
Week 2395246 1789120 1728239 54215 5808 641 457727
Servers Status Mail
Host Mode License MTA Uptime Load Averages TBA Queued Deferred Total
lt203 Primary Ok Running 3:20 2.81, 1.96, 1.61 - 0 7003 7003
lt206 Secondary Ok Running 14 days 3.61, 3.58, 3.75 - 0 13255 13255
lt207 Client Ok Running 14 days 3.24, 2.57, 2.51 - 0 10435 10435
lt208 Secondary Ok Running 14 days 4.43, 3.86, 3.99 - 0 13090 13090
lt209 Client Ok Running 14 days 2.84, 2.84, 2.84 - 0 18292 18292
Totals: 0 62075 62075
Refresh
Show Recipients

Queue Replication

The *Queue Replication* feature enables mail queue replication and failover between two systems. In the event that the primary owner of a mail queue is unavailable, the mirror system can take ownership of the mirrored mail queue for delivery.

Queue replication actively copies any queued mail to the mirror system, to make sure that ,if one system should fail or be taken offline, the mirror system can take ownership of the queued mail and deliver it. If the source system successfully delivers the message, the copy of the message on the mirror server is automatically removed.

In the following diagram, *System A* and *System B* are configured to be mirrors of each other's mail queues.



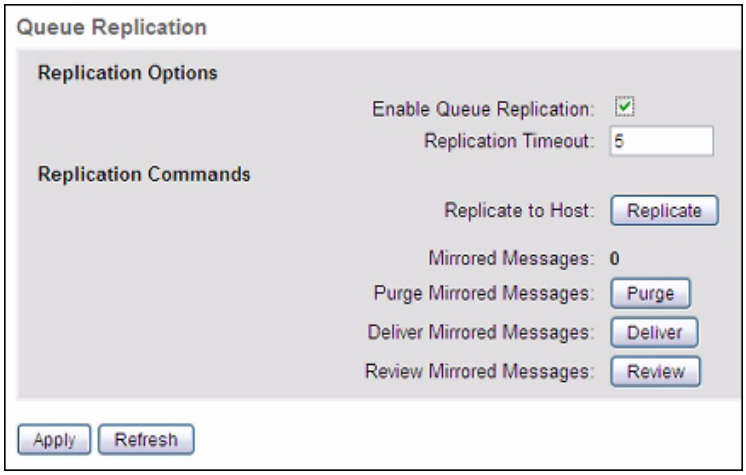
When a message is received by *System A*, it is queued locally and a copy of the message is also immediately sent over the failover connection to the mirror queue on *System B*.

If *System A* fails, administrators can login to *System B* and take ownership of the queued mail to deliver it. Messages are exchanged between the systems to make sure that the mirrored mail queues are correctly synchronized and to prevent duplicate messages from being delivered when a failed system has come back online.

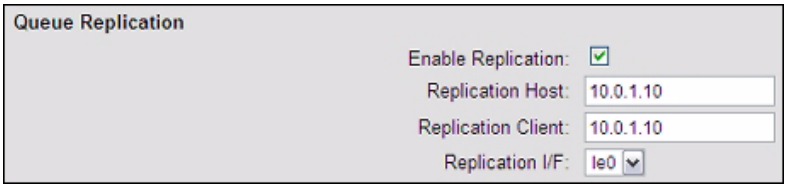
Configure Queue Replication

To configure queue replication:

1. Select **Administration > Multi-System Management > Queue Replication**.



2. Select the **Enable Queue Replication** check box.
3. Click **Apply**.
4. Select **Configuration > Network > Interfaces**.
5. Go to the **Queue Replication** section.
   The following options only appear in the Network settings screen after Queue Replication is enabled.



6. Select the **Enable Replication** check box.
7. Specify the **Replication Host** IP address of the host that will back up mail for this system.
   If you use Queue Replication in a cluster and use the interface connected to the cluster network for replication, specify the hostname of the host cluster system, such as SystemA, in the address: SystemA.example.com.
8. Specify the **Replication Client** IP address of the client that will back up its mail queue to this system.
   If you use Queue Replication in a cluster and use the interface connected to the cluster network for replication, specify the hostname of the client cluster system, such as SystemB, in the address: SystemB.example.com.
9. Select the **Replication I/F** (network interface) to use for queue replication.
   This network interface should be connected to a secure network. We recommend that queue replication and clustering functions be run together on their own dedicated subnet.

For example, because messages from *System A* are replicated on *System B*, enter the IP address for *System B* in the **Replication Host** field. *System A* also acts as a host for *System B*, so enter the address for *System B* in the **Replication Client** field.

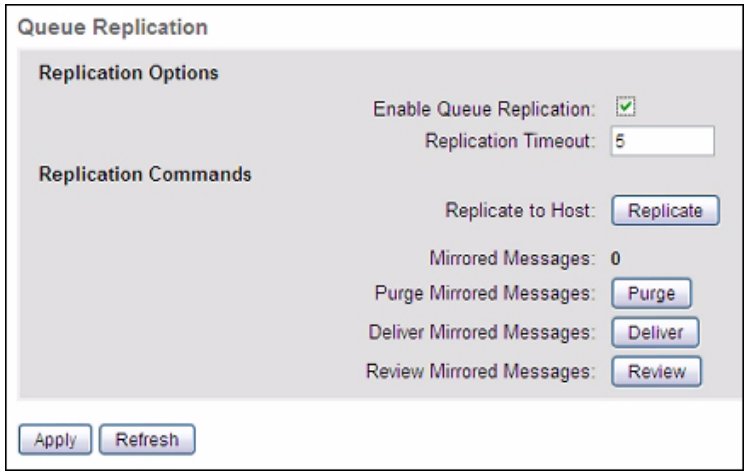
Messages from *System B* are replicated on *System A*, so enter the IP address for *System A* in the **Replication Host** field. *System B* also acts as a host for *System A*, so enter the IP address for *System A* in the **Replication Client** field.

Import and process mirrored messages

If you have two systems that mirror each other's mail queues and one of those systems fails, you must go to the mirror server and import the mirrored mail to make sure mail is correctly processed and delivered.

To import the mirrored messages:

1. Make sure that the host system is unavailable.
   Before you import any mirrored mail, you must make sure that the host system is not processing mail. If you import and process the mirrored mail on the mirror system, this can result in duplicate messages if the host system starts to work again.
2. On the mirror server, select **Administration > Multi-System Management > Queue Replication**.



3. Click the **Review** button to see the current mirrored mail.
4. Click **Deliver**.
   This system takes ownership of any queued mail mirrored from the source server, and processes and delivers it.

14 Web Scanning

Web Scanning Overview

The Web Proxy allows the system to manage web traffic and control access to external web sites. The system uses a subset of the same scanners that examine email messages to inspect the content of web traffic and file transfers. With the XCS policy features, you can apply web access policies to different users, groups, and domains. The Web Proxy analyzes client requests and allows or blocks access to specific web sites based on the configured access policies.

Web content inspection

The Web Proxy inspects downloaded and uploaded content with the following scanning features:

- **Kaspersky Anti-Virus** — Scans for viruses in downloaded and uploaded files.
- **URL Block Lists** — Blocks access to web sites that appear on a URL Block List.
- **Objectionable Content Filter (OCF)** — Scans web traffic for objectionable content based on a dictionary of blocked words and phrases.
- **Attachment Control** — Allows or blocks specific file MIME types.
- **Content Scanning** — Allows or blocks files based on specific text content within a file.
- **URL Categorization** — Blocks web sites based on a list of blocked web site content categories.
- **HTTP Blocked Sites List** — Blocks web sites based on a configurable list of web sites managed by the administrator.

The XCS cannot perform content inspection on HTTPS traffic.

You can configure a different action for each scanner, such as **Reject** (default) to reject the request, or **Just Log** to allow the request and send a log message to the Web Proxy log file.

Traffic Accelerator

The expansive growth of large interactive and collaborative web sites that are media intensive requires greater bandwidth, which can overload corporate networks.

The WatchGuard Traffic Accelerator solution provides several Web traffic enhancements to reduce bandwidth consumption, server loads, and network latency. This can result in better network performance and availability. The WatchGuard Traffic Accelerator includes the following features:

- **Web Caching** — The Web Caching feature of the WatchGuard Traffic Accelerator solution provides temporary storage of web data to enable faster retrieval of Web sites. This feature reduces bandwidth consumption and improves performance for subsequent accesses of these web sites because the data and images are read from the disk cache.
- **Streaming Media Bypass** — To manage streaming media traffic, the WatchGuard Traffic Accelerator can bypass streaming media content to reduce the strain on bandwidth resources.
- **Download and Upload File Limits** — Use the WatchGuard Traffic Accelerator's management and policy settings for file uploads and downloads to block or bypass files when the limits are exceeded. This prevents large files uploads and downloads that limit network bandwidth.

Automatic client web proxy configuration

Organizations that want to enforce the use of a proxy policy without the need to manually configure each individual browser can use the following methods for automatic proxy configuration:

- **Proxy Auto-Config (PAC) file** — A Proxy Auto-Config (PAC) file defines how a web browser can automatically choose an appropriate proxy server to connect to. The PAC file is a script file that browsers read and execute to determine which proxy to use.
- **Web Proxy Autodiscovery Protocol (WPAD)** — The Web Proxy Autodiscovery Protocol (WPAD) is supported by most web browsers to locate a Proxy Auto-Config (PAC) file automatically and then use this information to configure the browser's web proxy settings. The protocol can use DHCP or DNS to locate the PAC file.

Web Proxy best practices

The following notes describe some best practices to follow when you implement the Web Proxy for the first time.

- We recommend that you run the system for at least 24-48 hours with minimal scanning enabled before you enable threat and content control scanning on web traffic. This allows the web cache to populate and increases performance. After this initial period, enable threat and content control scanners as required.
- Enable DNS cachine to increase Web Proxy performance. This is enabled by default in **Configuration > Network > Interfaces**.
- Make sure that the **Large MTU** setting is enabled on the network interface designated for HTTP Proxy access.
- When you configure the Web Proxy in Transparent Mode, make sure that the **Large MTU** setting is enabled on the network interface configured as the **Bridge In** interface. You must enable the HTTP Proxy and reboot the system before you can enable bridging and Transparent Mode on the network interfaces.
- Make sure that your local DNS server is configured and is operational. Misconfigured DNS services and domain name translation issues can significantly decrease Web Proxy performance or cause the Web Proxy to stop working.

- If you enable the URL Categorization feature, it can take several minutes for the initial URL Categorization Control List to download. While the Control List downloads, HTTP traffic is not processed and users can receive policy error messages when web browsing. When the update is complete, HTTP traffic processing resumes. We recommend that you do not start processing HTTP traffic until this initial download process is complete.

Web Proxy support and limitations

The Web Proxy supports the following types of requests:

- HTTP 1.0 and 1.1
- HTTP pipelining
- HTTP keep-alive messages

The following list shows current limitations with the Web Proxy:

- HTTPS traffic is scanned by the proxy, but the content cannot be decrypted, scanned, or analyzed.
- FTP over HTTP is not supported with the Web Proxy.
- Clustering is not supported in Transparent Mode. A Web Proxy configured in Transparent Mode can be clustered with a non-Web Proxy system, such as a WatchGuard XCS system that processes email.

Web Deployments

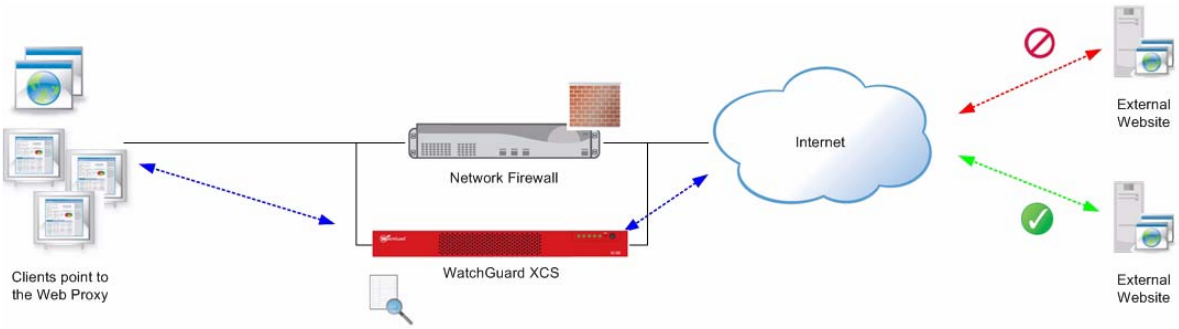
The following sections describe several different deployment models for the Web Proxy.

Full proxy parallel deployment

The Web Proxy can be deployed in parallel with an existing network firewall. To do this, you use two network interfaces. The HTTP ports (such as port 80) must be closed off to end clients by the network firewall to prevent them from circumventing the proxy.

Web clients must be manually reconfigured to use the system as their web proxy, such as hostname.example.com:8080. Otherwise, you must use proxy auto-discovery or other HTTP traffic redirection with routers or traffic manager devices.

The Full Proxy Parallel Deployment is the recommended Web Proxy deployment model.



Advantages

- Requires no additional performance overhead on the Web Proxy as it only processes web traffic
- Simple to deploy and troubleshoot connection issues
- System is located securely outside of the internal network
- System can be clustered with another WatchGuard XCS running web or email
- Automated failover with no network downtime

Disadvantages

- Must set up Proxy auto-discovery with PAC Files/WPAD to point to the WatchGuard XCS

Internal network deployment

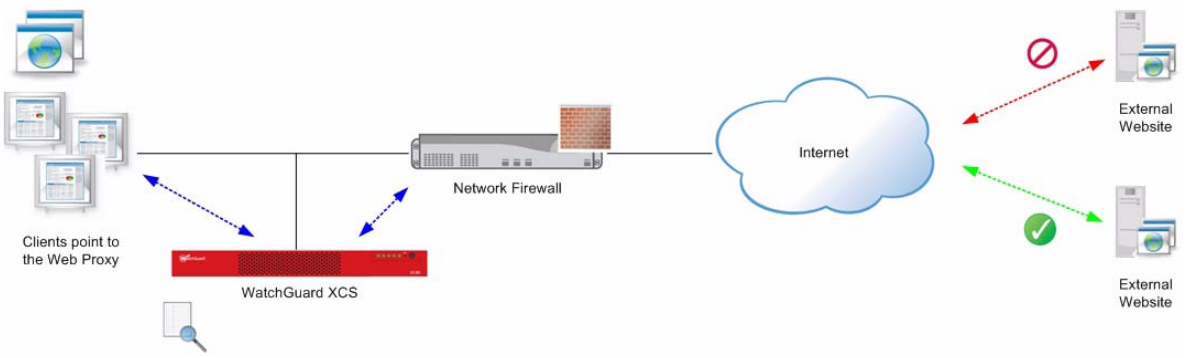
The Web Proxy can be deployed on the internal network connected with one network interface. The firewall must block HTTP traffic to prevent network clients from circumventing the proxy. These ports must be opened up for the Web Proxy only. Each internal client must be manually reconfigured to use the system as their web proxy, such as hostname.example.com:8080. Otherwise, you must use proxy auto-discovery or other HTTP traffic redirection with routers or traffic manager devices.

Advantages

- Requires no additional performance overhead on the system
- Simple to deploy and troubleshoot connection issues

Disadvantages

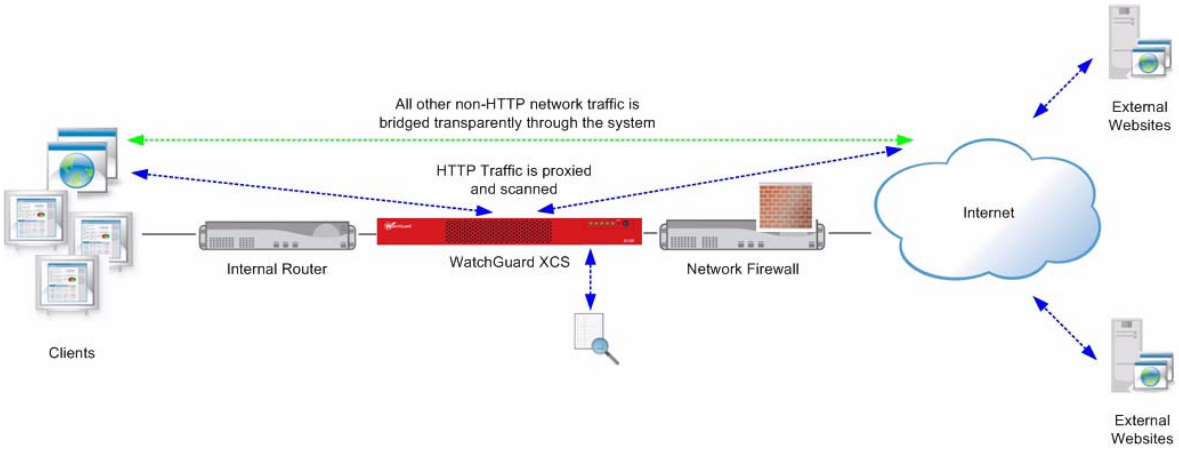
- Must set up proxy auto-discovery using PAC Files/WPAD to point to the WatchGuard XCS



Transparent mode deployment

The Web Proxy offers a Transparent Mode to integrate the system more easily into existing environments with minimal network reconfiguration. This method requires no network reconfiguration and the implementation is transparent to clients.

In a typical Transparent Mode implementation, the Web Proxy system is installed between the primary internal switch or router and an existing network firewall. It acts as a bridge for all non-local traffic, except selected web traffic that is examined by the Web Proxy. The system listens for web traffic on port 80 and any specific HTTP requests are processed by the Web Proxy for security threat processing and content filtering before the request is allowed through.



Advantages

- Offers a simple and seamless deployment. No network or client system reconfiguration is required.

Disadvantages

- All network traffic is sent through the Web Proxy, which you may not want, depending on the network environment.
- Packet inspection is performed on all traffic to determine if data should be proxied or bridged, which can potentially add additional performance overhead on the Web Proxy.
- The default port for HTTP traffic (port 80) cannot be modified in Transparent Mode.
- Only IP-based Proxy or Portal authentication can be used when in Transparent Mode.
- Clustering with other Web Proxy systems is not supported in Transparent Mode. A Web Proxy running in Transparent Mode can be clustered with a non-Web Proxy system, such as a WatchGuard XCS system processing email.
- If the system fails, all network traffic is stopped.

15 Available Resources

Available Resources

For additional information about the WatchGuard XCS and other WatchGuard products, please visit the following online resources.

Product Documentation
You can view and download the most current documentation for the WatchGuard XCS on the WatchGuard Product Documentation page:

http://www.watchguard.com/help/documentation

Training Resources
Training presentations and additional training resources are available on the WatchGuard Product Training page:

http://www.watchguard.com/training/courses.asp

WatchGuard User Forum
The WatchGuard forum is an interactive online user forum moderated by senior support engineers. Visit the WatchGuard XCS forum at:

http://www.watchguard.com/forum

Knowledge Base
You can view and search the knowledge base for information on specific WatchGuard product issues at:

http://watchguard.custhelp.com

WatchGuard Products and Services
For more information on WatchGuard products and services, visit the WatchGuard product information page:

http://www.watchguard.com/products